The Legal Limitations on Defending the National Information Infrastructure Against a Cyber Attack

Submitted to

Professor Ray Nimmer
Professor Paul Janicke
Professor Jordan Paust

By

Joe Dhillon

In fulfillment of
The Thesis Requirement

For Completion of the Master of Laws Program

At

The University of Houston Law Center

May 27, 1999

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	5.Dec.99	THESIS

4. TITLE AND SUBTITLE
THE LEGAL LIMITATIONS ON DEFENDING THE NATIONAL INFORMATION INFRASTRUCTURE AGAINST CYBER ATTACK

5. FUNDING NUMBERS

6. AUTHOR(S)
LT COL DHILLON JOGINDER S

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
UNIVERSITY OF HOUSTON

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
THE DEPARTMENT OF THE AIR FORCE
AFIT/CIA, BLDG 125
2950 P STREET
WPAFB OH 45433

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
FY99-436

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited distribution
In Accordance With AFI 35-205/AFIT Sup 1

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

14. SUBJECT TERMS

15. NUMBER OF PAGES
87

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT

> Security is no longer defined by armed forces standing between the aggressor and the homeland. The weapons of information warfare can outflank and circumvent military establishments and compromise the common underpinnings of both U.S. military and civilian infrastructure, which is now one and the same.
>
> *Center for Strategic and International Studies*

I. Introduction

It is hardly controversial to suggest that the explosion of new information technologies over the past ten years has had a profound impact on our society. The law has not been immune to these changes. The pillars of our jurisprudential framework, from contracts to criminal law, from the Constitution to the Copyright Act, have been subjected to the pressure of forces seeking an accommodation for the myriad technical and societal changes spawned during the Information Age. Not surprisingly, clear and compelling answers to the various legal issues raised by emerging technologies are lagging far behind the development of the technologies and their applications. Nonetheless, the potential commercial rewards for successful innovators have led many to enter the marketplace notwithstanding the risks associated with legal uncertainty.

The rewards for innovation and the risks of acting in the absence of clear legal authority are quite different in the realm of national security. The consequences of failure to act can be catastrophic. On the other hand, unlike actors in the commercial marketplace, governmental actors arguably have a duty to ensure that their policies and conduct are consistent with the letter of our laws

and the spirit of our democratic values. In other words, the lack of an obviously red light should not necessarily mean go. Creative short-term legal "solutions" are fraught with risk. These risks are particularly evident where the singularly important governmental responsibility of providing for national security appears to collide with the individual rights and liberties that have been the defining characteristics of American society for over two hundred years.

The purpose of this paper is to examine the selected domestic and international legal limitations the ability and authority of the United States Air Force to carry out its unique role in ensuring the security of this country against cyber attacks upon our critical information infrastructures.

Section II, "Critical Infrastructures and Information Technology," will briefly describe the technical context in which these legal issues have arisen. This section will present a brief history of the Internet and a description of the National Information Infrastructure (NII) that encompasses network and other computer and telecommunications technologies. The discussion of the NII will describe how many critical components of our society--from transportation to banking to energy--are dependent upon the NII and how this dependence translates into vulnerability.

In order to remove any lingering doubts about the scope and immediacy of our vulnerability, the next section presents examples of actual and simulated "cyber attacks" against commercial and military targets.

Section IV, "Legal Analysis," is the heart of the paper. It describes and examines the significant constitutional and statutory provisions as well as norms of customary international law that affect the ability and authority of the Air Force to respond to cyber attacks on our critical commercial and defense infrastructures. In particular, the paper will examine the Fourth Amendment, the various provisions of what began as the Federal Wiretap Act, (18 U.S.C. §§ 2510-2711, as amended), the Foreign Intelligence Surveillance Act (50 U.S.C. §§ 1801 et seq.), the Posse Comitatus Act, and international norms regarding the use of force. The purpose of this section is to analyze the pertinent law in order to identify the legal limitations on Air Force action.

II. Critical Infrastructures and Information Technology

A. What is the National Information Infrastructure?

> Life is good in America because things work. When we flip the switch, the lights come on. When we turn the tap, clean water flows. When we pick up the phone, our call goes through. We are able to assume that things will work because our *infrastructures* are highly developed and highly effective.[1]

On July 15, 1996, President Clinton issued Executive Order 13010, establishing the President's Commission on Critical Infrastructure Protection (PCCIP). Infrastructures are societal substructures that are essential to the viability of the nation, such as "roads, schools, power plants, transportation and communication systems, etc."[2] PCCIP was charged with assessing the

---

[1] Critical Foundations; Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection (Critical Foundations), 1997, at page 3.
[2] Webster's New World Dictionary, Third Edition, 1988, at page 694.

vulnerabilities of eight specified critical infrastructures to physical and cyber threats. The following infrastructures were identified as critical: transportation; oil and gas production and storage; water supply; emergency services; government services; banking and finance; electrical power; and, information and communications.[3] These critical infrastructures constitute the essence of what makes America among the most materially advanced societies on earth.

With regard to the threat of a physical attack using traditional kinetic means of destruction, "the physical breadth of the infrastructures made it difficult for a potential malefactor to cause anything other than an isolated disturbance."[4] However, the dependence of each infrastructure on computers, advanced telecommunications, and the Internet for the most basic control and management of the various operations within an infrastructure, as well as for increasingly efficient interaction with other infrastructures, has dramatically increased the vulnerability of all critical infrastructures to cyber attack.[5] Moreover, the reliance of each of the critical infrastructures upon a single, publicly accessible, information infrastructure increases the extent of cumulative

---

[3] Critical Foundations at 4.

[4] Michael Vatis, Chief, National Infrastructure Protection Center, Federal Bureau of Investigation, Prepared Statement to the Joint Economic Committee, March 24, 1998, at page 2, Federal Information Systems Corporation, Federal News Service.

[5] "[E]lectric power grids and natural gas pipelines are controlled by computer systems, and those computers may be linked to each other and to the company headquarters by publicly accessible telecommunications systems and commercially available information technologies to allow efficient management of power generation and smooth delivery to consumers. Billions of shares are traded each day over the telephone or Internet, and the stock exchanges could not function today without their vast networks of computers. Banks no longer rely on ledger books and safe deposit boxes to account for and secure their holdings, but depend on computerized accounting systems to manage depositors' accounts. The telecommunications system itself no longer uses operators to manually plug in calls to a switchboard but depends on computerized switching

societal harm that can be wrought through an effective cyber attack against the information infrastructure.

> Technologies and techniques that have fueled major improvements in the performance of our infrastructures can also be used to disrupt them. The United States, where close to half of all computer capacity and 60 percent of Internet assets reside, is at once the world's most advanced and most dependent user of information technology. More than any other country, we rely on a set of increasingly accessible and technologically reliable infrastructures, which in turn have a growing collective dependence on domestic and global networks. This provides great opportunity, but it also presents new vulnerabilities that can be exploited. It heightens the risk of cascading technological failure, and therefore of cascading disruption in the flow of essential goods and services.[6]

B. The Internet

The critical component of the information infrastructure is the Internet. "The Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks."[7] It facilitates the exchange of large quantities of data and other information over long distances, at low cost, in a generally reliable manner. The Internet also permits public access to the information. This creates the very dangerous possibility that the flow of critical information could be disrupted or the content manipulated.

---

stations to handle the billions of calls placed each day. The government also relies on computers and publicly available communications systems to conduct the nation's business." *Id.*

[6] Critical Foundations, at 5.

[7] *American Civil Liberties Union v. Janet Reno*, 929 F.Supp. 824, 830 (E.D. PA 1996)

The technological breakthrough that fostered the development of the Internet came from research conducted by the Defense Advanced Research Projects Agency (DARPA).[8] In the late 1960's and early 1970's, DARPA scientists conceived of packet switching networks. Essentially, this technology enabled the exchange of information between computers in short bursts of data called "packets." Prior to the advent of packets, the communications links between the computers involved in an exchange of information were dedicated to the exclusive use of those particular computers. This was an extremely inefficient use of communications resources. Not only did a system design based on dedicated communications links actually increase the possibility of an erroneous transmission, it did not reflect the fact that the actual exchange of even large amounts of information between computers is accomplished in short discrete bursts.[9]

The DARPA scientists conceived of a method of labeling the digital packets so that the information could be transferred to a single destination along a number of different routes but still be reconstructed in the proper order regardless of the sequence of actual transmission.[10] Moreover, they established the viability of this technology over satellite and other wireless networks.[11] By

---

[8] Dr. Robert E. Kahn, President, Corporation for National Research Initiatives, Statement to the Senate Committee on the Judiciary, November 4, 1997, Federal News Service.
[9] *Id.*
[10] *Id.*
[11] *Id.*

eliminating the need for dedicated links between computers, packet switching networks dramatically decreased the costs of establishing computer networks.[12]

Some estimates place the number of people who will have Internet access by the year 2000 at 1 billion.[13] Touted as the "Information Superhighway," the Internet enables any of the people capable of entering it with previously unimagined access to increasingly sensitive information. The pressure to quickly develop and capitalize upon the commercial opportunity afforded by the Internet has exceeded the need to regulate, or otherwise ensure the security of, operations that rely upon benefits afforded by the Internet. Until now.

C. Access/Vulnerability: Two Sides of the Same Coin

> We have spent years making systems interoperable, easy to access, and easy to use, yet we still rely on the same methods of security that we did when data systems consisted of large mainframe computers housed in closed rooms with limited physical access. By doing so, we are building an information infrastructure, the most complex the world has ever known, on a very insecure foundation.

---

[12] *Id.*

[13] "Estimates that there will be over 1 billion users on the Internet by 2000 underscores the importance of establishing trust and security in a highly distributed, network-centric computing environment such as the Defense Information Infrastructure (DII)." Arthur L. Money, Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Testimony Before the House Armed Services Committee, Subcommittee on Military Procurement, Military Research and Development, February 23, 1999, Federal News Service. "The nature of the Internet is such that it is very difficult, if not impossible, to determine its size at a given moment. It is indisputable, however, that the Internet has experienced extraordinary growth in recent years. In 1981, fewer than 300 computers were linked to the Internet, and by 1989, the number stood at fewer than 90,000 computers. By 1993, over 1,000,000 computers were linked. Today, over 9,400,000 host computers worldwide, of which approximately 60 percent located within the United States, are estimated to be linked to the Internet. This count does not include the personal computers people use to access the Internet using modems. In all, reasonable estimates are that as many as 40 million people around the world can and do access the enormously flexible communication Internet medium. That figure is expected to grow to 200 million Internet users by the year 1999." *ACLU v. Reno*, 929 F.Supp. at 830.

> An article in China's People's Liberation Daily stated that . . . "an adversary wishing to destroy the United States only has to mess up the computer systems of its banks by high-tech means. This would disrupt and destroy the U.S. economy." If we overlook this point and simply rely on the building of a costly standing army, it is just as good as building a contemporary Maginot Line.[14]

The Federal Bureau of Investigation (FBI) estimates that the cost of electronic crimes exceeds $10 billion per year.[15] The problem is hard to pin down for a variety of reasons. A victim may not be immediately aware that it has been attacked. And, even if the company becomes aware of the attack, it may choose not to make any public disclosure about an apparent vulnerability in its computer security. Approximately only one company in six that is victimized by cybercrime reports such losses to law enforcement agencies.[16] In a single well-publicized incident, a group of Russians stole $10 million from Citibank by

---

[14] George Tenet, Director, Central Intelligence Agency, Testimony to the Senate Governmental Affairs Committee, June 24, 1998, Federal News Service. [Although I was unable to verify Mr. Tenet's citation to the original source, I did find another reference: "China's army newspaper, Jiefangjun Bao, in a March 24, 1998 article emphasized the need "to learn to launch an electronic attack on an enemy and ensure electromagnetic control in an area and time favorable to us. . . . In a system confrontation, we should lean to conduct a structural analysis and study ways of structural sabotage." Military and C4I, infowar. com, dated October 22, 1998. <http://www.infowar.com/mil_c4i/mil_c4i_122298a_j.shtml>]

[15] Cybercrime . . . Cyberterrorism . . . Cyberwarfare . . .Averting an Electronic Waterloo (Electronic Waterloo), Center for Strategic and International Studies, 1998. "The U.S. today faces a new and unprecedented threat: strategic information warfare. There is now the potential for a dedicated, sophisticated adversary to conduct coordinated strikes against the computers, communications systems, and databases that underpin modern society. This is not mere hacking or computer crime; rather the objectives are geopolitical and economic. And traditional national security measures will be ineffective. . . . This report assess that threat and points the way towards practical responses." <http://www.csis.org/pubs/cyberfor.html>

[16] *Id.*

gaining access to the bank's computer network.[17] In addition to the direct loss of funds, the news of the loss itself was used by competitors to put fear in the minds of the some of Citibank's clients in an effort to win their business.[18] This experience has been used to justify the reluctance of many businesses to report computer intrusions.

Notwithstanding their cumulative economic harm, individual electronic crimes are not necessarily issues of national security. The more significant concern to the Air Force is attacks that are motivated by a desire to harm the national security interests of the United States. Such cyber attacks may be designed to accomplish some symbolic end, as is usually the case with acts of terrorism, or may be motivated by a desire to diminish our ability to execute a military response to other activity by the attacker elsewhere in the world that is adverse to our national interests.

As noted above, the increased reliance upon the information infrastructure has made each of the critical infrastructures more vulnerable to attack. For instance, the energy industry has developed Supervisory Control and Data Acquisition (SCADA) systems that permit the remote monitoring and control of energy production and distribution systems.[19] The downside of these Internet dependent management tools is an increased vulnerability to serious damage

---

[17] "Cyber threats are all too real: Governments fail to comprehend information warfare", National Post, February 20, 1999, at page D3.
[18] *Id*
[19] Critical Foundations: Protecting America's Infrastructures, at page 12.

and disruption caused by a cyber attack.[20] The banking and finance infrastructure is similarly dependent on the ability to reliably exchange information through the Internet.[21] The Director of Central Intelligence, George Tenet, offered the following assessment of our vulnerability to, and likelihood of, cyber attack:

> [P]otential attackers range from national intelligence and military organizations, terrorists, criminals, industrial competitors, hackers, and disgruntled or disloyal insiders. Any why would we be attacked? There are plenty of incentives. Trillions of dollars in financial transactions in commerce, moving over a medium with minimal protection, and sporadic law enforcement. Increasing quantities of intellectual property residing on network systems, and the opportunity to disrupt military effectiveness and public safety with the elements of surprise and anonymity. The stakes are enormous. Protecting our critical information infrastructure is an issue we should all be deeply troubled about.[22]

Cyber attacks may be directed against critical aspects of the NII or against the over two million computers, 10,000 local networks, and 100 long-distance networks that directly support the Department of Defense's (DoD) mission effectiveness and operational readiness.[23] "Despite the existence of dedicated military communications satellites, more than 95 percent of military

---

[20] *Id.*
[21] *Id.*
[22] George Tenet, Director, Central Intelligence Agency, testimony before the Senate Governmental Affairs Committee, June 24, 1998, Federal News Service.
[23] *Information Security--Computer Attacks at Department of Defense Pose Increasing Risks*, General Accounting Office, Report to Congressional Requesters (GAO/AIMD-96-84) May 1996, at page 12. (available at <http://epic. org/security/GAO_DOD_security.html>)

communications travels via the commercial telephone networks."[24] This collection of telecommunications and information systems is known as the Defense Information Infrastructure (DII).

The DII is a prime target of cyber attacks. Deputy Secretary of Defense John Hamre recently testified that the DII is the target of approximately 80-100 intrusions each day, approximately 10 of which require detailed investigation.[25] Even more sobering than the apparent number of intrusions is the information that can be gleaned from the Defense Information Systems Agency's (DISA) Vulnerability Analysis and Assessment Program about the ease of penetrating the DII and the likelihood of doing so without detection. The vulnerability assessment program is essentially an ongoing internal audit of the security of the DII.[26] Because it is an internal audit, the program allows us to determine the effectiveness of our defensive and reporting measures. Over the course of 38,000 attacks on the DII conducted pursuant to this program, DISA was able to successfully gain access to the target system 65 percent of the time.[27] Of the attacks that were successful, only approximately 4 percent were detected.[28] Moreover, only 27 percent of these were reported to DISA.[29] In other words,

---

[24] A Primer on Legal Issues in Information Operations, Department of the Air Force, undated, at page 4. (A copy on file with the author.)
[25] Testimony of Deputy Secretary of Defense John Hamre before the Senate Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, March 16, 1999.
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*

only 1 in 150 successful attacks were handled in the manner necessary to prompt an active defensive response.[30]

Almost certainly, the figure of 80-100 intrusions per day overstates the actual extent of harmful cyber activity directed at the DII. It is likely that the vast majority of these intrusions are inadvertent, or reflect the efforts of hackers who simply desire to test their skills against what they perceive to be a formidable challenge.[31] "[Hackers] see the Department of Defense as . . . the big banana. The final exam. The ultimate challenge . . . to test their skills."[32]

Nonetheless, the vulnerability of our infrastructures, coupled with the undeniable reality that there are those who wish to harm the United States, militates in favor of the conclusion that a cyber attack against our information infrastructure presents a real, and current, threat to our national security.[33]

---

[30] However alarming these figures may be, they are consistent with, or compare favorably to, information about the security of private sector computer networks. "Consider the following report by Robert Ayers, Chief of the Center for Information Systems Security. Mr. Ayers' group recently used readily available hacker tools freely available on the Internet to test the vulnerability of U.S. systems. He found that:

> 88% of the time they are effective in penetrating the system,
> 96% of all system penetrations are undetected, and
> 95% of the instances where penetration is detected, nothing is done."

Matthew G. Devost, National Security in the Information Age, A Thesis Presented to The Faculty of the Graduate College of The University of Vermont, May 1995, at page 16. <www.terrorism.com/documents/devostthesis.html>

[31] Michael Vatis, Chief, NIPC, Senate Testimony June 10, 1998.

[32] *Id.*

[33] "There is mounting evidence that attacks on [Department of Defense (DoD)] computer systems pose a serious threat to national security. Internet connections make it possible for enemies armed with less equipment and weapons to gain a competitive edge at a small price. As a result, this will become an increasingly attractive way for terrorist or adversaries to wage attacks. . . . In some extreme scenarios, studies show that terrorists or other adversaries could seize control of [DoD] information systems and seriously degrade the nation's ability to deploy and sustain military forces. Official estimates show that more than 120 countries already have or are

III. Incidents of Actual/Simulated Cyber Attacks

Even among those with an above average knowledge of computer networks, the notion of a cyber attack against our critical national infrastructures still seems a bit abstract. Before delving into an esoteric analysis of the legal limitations on responding to such an attack, let's consider some examples of actual and simulated cyber attacks in order to provide some context for the ensuing discussion of legal theory.

The backbone of our information infrastructure is our system of public telephone networks. Our recent history is full of examples of our extensive dependence on these networks and the financial costs and societal consequences of even a short-term outage. "In 1992, a failed AT&T switching station in New York put both Wall Street and the New York Stock Exchange out of business for an entire day . . . . The failure resulted in 4.5 million blocked domestic long distance calls, nearly 500,000 interrupted international calls, and the loss of 80 percent of the Federal Aviation Administration's circuits."[34] To the extent that Wall Street is one of the most venerated symbols of our capitalistic society, the value to an adversary of stopping the market's activities is far greater than simply the economic disruption that ensues.

Immediately after the terrorist attack on the World Trade Center, the telecommunications network that serves lower Manhattan was overwhelmed with

---

developing such computer attack capabilities." *Information Security--Computer Attacks at Department of Defense Pose Increasing Risks*, General Accounting Office, May 1996, at 5.

[34] Bowman, Stephen, *When the Eagle Screams: America's Vulnerability to Terrorism*, Carol Publishing Group, New York, 1994, at page 155.

calls from those who were concerned about the effects of the bombing.[35] "The phone lines in lower Manhattan were effectively jammed, and some commercial banks, who had to close out their daily transfers in order to prevent a financial crisis, were required to use microwave communications to do it."[36]

In March 1997, the vulnerability created by our dependence on an insecure telecommunications infrastructure was highlighted by the actions of a teenage hacker using a simple personal computer. The hacker gained access to and disabled the local loop carrier in central Massachusetts. A local loop is a computer that translates multiple data and voice lines into a single fiber connection.[37] By disabling the local loop, the hacker shut down telephone service in the entire geographic area served by the connection.[38]

In this case, the victims were the 600 residents of Rutland, Massachusetts who lost all phone service, including 911 emergency service.[39] In addition, the loss of telephone service adversely affected the safety of local air traffic. "[The]

---

[35] Giovagnoni, Robert E., PCCIP General Counsel, *Framing the Issues: An Overview*, A Presentation to the Center for Law, Ethics, and National Security at Duke University, April 1998, page 1.

[36] *Id.*

[37] "In many respects, a loop carrier system serves the same function as a circuit breaker box in a home or an apartment. Individual wires do not run from each plug or light in a home or an apartment to the electric company. Rather, the myriad of plugs and lights are connected to a circuit breaker box in a corner of the home or apartment, to which the electric company attaches a single, efficient cable. If the circuit breaker box is disabled, however, none of the lights and outlets in the house can function. Loop carrier systems are used by telephone companies to integrate service provided over hundreds of telephone lines for digital transmission over a single, high capacity fiber-optic cable to a central office." Department of Justice Press Release, "Juvenile Hacker Cuts Off FAA Tower," March 18, 1998.
<http://www.usdoj.gov/criminal/cybercrime/juvenilepld.htm>

[38] Danahy, Jack, Director of Engineering, GTE Internetworking, *Framing the Issues, Some Examples*, A Presentation to the Center for Law, Ethics, and National Security at Duke University, April 1998, page 2.

[39] *Id.*

same telephone service provides the primary mechanism for the nearby Worcester Airport to transmit radio signals from aircraft to the tower. The same failure caused the air traffic control tower to be unable to printout progress of incoming and passing aircraft."[40]

It took Bell Atlantic technicians two hours to discover the security breach and six hours to bring the system back into full operation.[41] However, it took a year for Bell Atlantic to develop and implement security countermeasures.[42] Had the target of the attack been a more critical node in the telecommunications infrastructure, the consequences would certainly have been more severe.

The hacker was the first juvenile to face criminal computer fraud charges. He entered a guilty plea. His sentence included restitutionary payments to Bell Atlantic, forfeiting his computer equipment, and performing community service.[43]

The DII has also been the subject of cyber attacks. The attackers "have stolen, modified, and destroyed both data and software. . . . They have shut down entire systems and networks, thereby denying service to users who depend on automated systems to help meet critical functions."[44]

From March through May 1994, two hackers made more than 150 intrusions into the computer network at an Air Force research and development facility in Rome, New York. Rome Laboratory is the Air Force's primary facility for conducting research into advanced command and control systems. Because

---

[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*

it works with academia, commercial developers and other DoD entities in pursuing research into such areas as artificial intelligence, the laboratory is connected to, and a very intensive user of, the Internet.[45]

The hackers were located in Great Britain. However, as is typically the case in cyber attacks, they arrived at their target indirectly. In this case, they reached Rome Laboratory only after making a variety of connections in South America, and throughout the United States. It was five days before the attack was detected by the Air Force.[46]

> The attackers were able to seize control of Rome's support systems for several days and establish links to foreign Internet sites. During this time, they copied and downloaded critical information such as air taking order systems data. By masquerading as a trusted user at Rome Laboratory, they were able to successfully attack systems at other government facilities, including the National Aeronautics and Space Administration (NASA) Goddard Space Flight Center, Wright-Patterson Air Force Base, some Defense contractors, and other private sector organizations.[47]

While the costs of the attack to the Air Force have been estimated at $500,000, the potential national security impact of such an attack is difficult to quantify but certainly much more significant. For instance, the hackers may have installed "malicious code in software which could be activated years later,

---

[44] GAO, Information Security, at page 13.
[45] *Id.*
[46] Pirog, John, *Rome Lab Break-in*, A Presentation to the Legal Aspects of Information Operations Symposium at the Air Force Judge Advocate General's School, October 20, 1998. (Copy on file with author.)
[47] GAO, Information Security, at page 13.

possibly jeopardizing a weapons system's ability to perform safely and as intended. . . ."[48]

In June 1997, the Joint Chiefs of Staff initiated a no-notice military exercise named "Eligible Receiver." The purpose of the exercise was to test the ability of the DoD, and various other governmental agencies, to respond to coordinated cyber attacks against critical aspects of the NII and DII. More specifically, the exercise scenario involved efforts by North Korea to conduct a terrorist campaign against various aspects of our infrastructure with the goal of hindering our ability to effectively conduct military operations on the Korean Peninsula.[49]

The real "enemy" during "Eligible Receiver" was a "Red Team" comprised of approximately 40 DoD employees. They were not computer experts but did have a working knowledge of information technology. (Those familiar with the operation believe that the specialized knowledge required to conduct such an attack is that possessed by "kids who have been playing on their computers.")[50] The software that they used to conduct their attack was limited to that which was available on the Internet. They were given approximately three months to prepare for the exercise.[51]

---

[48] *Id.*

[49] Peters, Whitten, Principal Deputy General Counsel, DoD, and Marshall, Richard, Office of the General Counsel, National Security Agency, "Defensive Information Operations", A Presentation to the Legal Aspects of Information Operations Symposium, Air Force Judge Advocate General's School, October 18, 1997, at page 5.

[50] Padgett Testimony.

[51] Padgett, Ellie, Deputy Chief, Office of Defensive Information Warfare, NSA, Testimony to the Subcommittee on Technology, Terrorism and Government Information, June 10, 1998, Federal Document Clearing House, Inc.

By all accounts, the attack was a success:

> [T]he hackers found it exceptionally easy to penetrate well-defended systems. Air traffic control systems were taken down, power grids made to fail, oil refineries stopped pumping--all initially apparent accidents. At the same time . . . [it] proved remarkably easy to disrupt the [DoD logistics] network both by changing orders so that, for example headlamps rather than missiles end up at a fighter squadron, and to interrupt the logistics flow by disrupting train traffic. . . .
>
> The result was a serious degradation of the Pentagon's ability to deploy and to fight. In other words, a team of hired hackers, using commercially available information and artificially constrained by the law and the rules of the game, had successfully shown that an electronic Pearl Harbor is not only possible today but could be completely successful.[52]

More recently, in February 1998, as the United States was preparing to exercise military force against Iraq, the Air Force Information Warfare Center detected a series of apparently coordinated intrusions into the DII. The intrusions were traced back through a number of different educational institutions and then to Abu Dhabi, United Arab Emirates.[53] The Joint Chiefs of Staff together with the FBI launched an intensive investigation to determine the source, extent, and nature of the intrusions. It was determined that the intruders were placing "trapdoors" in the computer networks that would subsequently allow them to enter without being detected.[54] "Although the

---

[52] Adams, James, *The Next World War: Computers are the Weapons and the Front Line is Everywhere,* Simon & Schuster, New York, (1998), at pages 187-88.
[53] Vistica, Gregory and Thomas, Evan, *The Secret Hacker Wars*, Newsweek, June 1, 1998, at page 60.
[54] *Id.*

systems being hit were unclassified. . . Pentagon officials worried that by tampering with the data, the hackers could disrupt military operations, especially the U.S. force buildup then occurring in the Persian Gulf. Unsure where the attacks were originating or how many hackers were involved, Deputy Defense Secretary John J. Hamre notified President Clinton early in the search that the intrusions might be the first shots of a genuine cyber war, perhaps by Iraq as it faced a renewed threat of U.S. airstrikes."[55]

Ultimately, the hacking was traced to Cloverdale, California. The attackers were two 16 year olds who were being assisted by an 18-year-old Israeli "mentor." The two Americans were sentenced to perform community service and refrain from accessing computers without proper supervision during a probationary period.[56]

Cyber attacks are continuing.[57] On March 5, 1999, CNN reported that DoD computers are under a coordinated and organized attack from hackers.[58] Representative Curt Weldon spoke to reporters after receiving a classified briefing from Deputy Secretary of Defense John Hamre. Weldon characterized

---

[55] *Id.*

[56] Van Derbeken, Jaxon, "Cloverdale Hackers Plead Guilty," *San Francisco Chronicle*, July 30, 1998, at page A18.

[57] See, e.g., Uhlich, Robert, "Connected: Hackers attack military satellite," *The Daily Telegraph* (London), March 4, 1999, at page 2. "A group of hackers suspected of seizing control of a British military communications satellite using a home computer, triggering a frenetic security alert, has been traced to the south of England. [T]he hackers found a "cute way" into the control system for one of the Ministry of Defence's Skynet satellites and "changed the characteristics of channels used to convey military communications, satellite television and telephone calls."

[58] "Hackers target Pentagon computers," <http://cnn.com>, (visited March 5, 1999)

the situation in no uncertain terms: "There is an attack under way. You can basically say we are at war."[59]

On April 10, 1999, the London Times reported of "growing fears that international markets could be destabilized by a 'cyber attack' from Serbian hackers. . .[who] are already known to be threatening the computer systems of Western companies, with utilities and financial institutions seen as prime targets. NATO and the U.S. Department of Defense have confirmed that their computer networks have been under a 'cyber attack' from Belgrade since last week."[60]

IV. Legal Analysis

The remainder of this paper analyzes the more significant legal limitations on the ability of the Air Force to respond to these threats. These limitations are found in the Fourth Amendment to the U.S. Constitution; the primary statutory provisions that impose restrictions on the monitoring of electronic communications; the Posse Comitatus Act; and customary international law regarding the use of force.

A. The Fourth Amendment

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. *U.S. Const. amend. IV.*

---

[59] *Id.*

[60] "Serb hackers pose threat to markets," *The Times* (London), April 10, 1999, business section.

The essential purpose of the Fourth Amendment is to place limits on the ability of the government to intrude upon the private aspects of the lives of the people, even where the government is ostensibly acting to protect the community by discovering evidence of unlawful activity. Its terms are not absolute but reflect an attempt to limit the government to the extent necessary to preserve individual autonomy and privacy without depriving the government of the authority to maintain public order.[61]

The Fourth Amendment contains two clauses. The first establishes the requirement that all searches that implicate a privacy interest be reasonable.[62] The second establishes the requirement that all warrants permitting such a search be based upon an independent determination of probable cause and specify, with particularity, the scope of the search.[63] The language of the amendment does not clearly establish the nature of the relationship between the two clauses. That is, it implies, but does not explicitly state, that a warrantless search is, by definition, unreasonable.

---

[61] "Civil liberties, as guaranteed by the Constitution, imply the existence of an organized society maintaining public order without which liberty itself would be lost in the excesses of unrestrained abuses." Cox v. New Hampshire, 312 U.S. 569, 574 (1941)

[62] See generally, Jennifer Y. Buffaloe, *"Special Needs" and the Fourth Amendment: An Exception Poised to Swallow the Warrant Preference Rule*, 32 Harv. C.R.-C.L. L. Rev. 529 (Summer, 1997) at 529, note 2. "Compare Jacob W. Landynski, Search and Seizure and the Supreme Court: A Study in Constitutional Interpretation 42 (1966) . . . with Akhil Reed Amar, Fourth Amendment First Principles, 107 Harv. L. Rev. 757, 801 (1994) (arguing that the 'core of the Fourth Amendment . . . is neither a warrant nor probable cause, but reasonableness.")"

[63] "Inherent in the concept of a warrant is its issuance by a 'neutral and detached magistrate.' *Coolidge v. New Hampshire*,[403 U.S. at 481]; *Katz v. United States*, [389 U.S. at 356]" *United States v. United States District Court for the Eastern District of Michigan*, 407 U.S. 297, 304 (1972)

The majority of Fourth Amendment jurisprudence reflects this understanding. "The firm rule until the late 1960's was that in order for a search to be 'reasonable,' law enforcement officials desiring to conduct a search must first obtain a warrant from a neutral and detached magistrate by establishing probable cause that a law had been violated."[64] However, as the Supreme Court has been required to apply the traditional principles of the Fourth Amendment in non-traditional contexts, the number of exceptions to this rule has grown.[65] This paper will analyze whether the actions of a national security organization taken in response to an actual or perceived cyber attack against private or public property falls into one of the existing exceptions.

Even more fundamental, however, is the issue of whether the owner or operator of a computer system has a privacy interest deserving of protection by the Fourth Amendment. In other words, does the language in the first clause about "persons, houses, papers, and effects" apply to computer networks? If so, how and to what extent? Interestingly, at approximately the same time that the Court began to expand on the list of exceptions to the warrant preference rule, it also began to acknowledge that new technologies permitted governmental

---

[64] Jennifer Y. Buffaloe, "Special Needs" and the Fourth Amendment: An Exception Poised to Swallow the Warrant Preference Rule, 32 Harv. C.R.-C.L. L. Rev. 529, 530 (Summer 1997) See *Almeida-Sanchez v. United States*, 413 U.S. 266, 277 (1973) (Powell, J., concurring) (But it is by now axiomatic that the Fourth Amendment's proscription of 'unreasonable searches and seizure' is to be read in conjunction with its command that 'no Warrants shall issue, but upon probable cause.")

[65] See Craig M. Bradley, Two Models of the Fourth Amendment, 83 Mich. L. Rev. 1468, 1473-74 (1985) (identifying 20 exceptions to the warrant preference rule); Elise Bjorkan Clare et al., Warrantless Searches and Seizures, 84 Geo. L.J. 743, 743 (1996) (13 categories of exceptions, including searches in which the special needs of law enforcement make the probable cause requirement impracticable).

agents to intrude upon a citizen's privacy in ways that did not resemble a traditional search.[66] In other words, the reach of these new technologies required a revised understanding of the notion of privacy. This paper will explore how Fourth Amendment privacy doctrine has been, and should be, applied in the context of computer networks.

1. Fourth Amendment Doctrine

Throughout much of American history, the Supreme Court has taken a literal interpretation of the first clause of the Fourth Amendment. "Unless government agents searched or seized tangible 'houses, papers, or effects,' Fourth Amendment protections failed to apply."[67] For instance, in 1928, the Court was presented with the question of whether wiretaps on phone lines implicated the privacy interests protected by the Fourth Amendment. The case, *Olmstead v. United States*, 277 U.S. 438 (1928), involved actions of federal prohibition officers to uncover evidence of a liquor importing conspiracy. The location of the wiretaps did not require the agents to enter onto the defendant's property. The Court decided that a Fourth Amendment search had not occurred. The lack of a physical entry onto the defendant's property was determinative of the Court's conclusion:

> Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a

[66] As discussed more fully below, in *Katz v. United States*, 389 U.S. 347 (1967), the Court recognized for the first time that the scope of a constitutionally protected expectation of privacy may encompass a search which does not involve a physical invasion of privacy.
[67] Michelle Skatoff-Gee, Changing Technologies and the Expectation of Privacy: A Modern Dilemma, 28 Loy. U. Chi. L.J. 189, 192 (Fall, 1996)

> defendant unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an *actual physical invasion* of his house or 'curtillage' for the purpose of making a seizure.[68] (emphasis added.)

Justice Brandeis wrote in dissent. He exhorted the Court to understand the language of the Fourth Amendment in terms of the broad principles it was designed to further.[69] Brandeis understood that privacy-invading technology would evolve in ways that the framers could not have foreseen.[70] His description of the reach of the Fourth Amendment is classic in its characterization of the right to be let alone as a singularly important characteristic of a civilized society.[71]

---

[68] *Olmstead v. United States*, 277 U.S. 438, 466 (1928)

[69] "Clauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world. It was with reference to such a clause that this Court said in *Weems v. United States*, 217 U.S. 349, 373: 'Legislation, both statutory and constitutional is enacted, it is true, from an experience of evils, but its general language should not, therefore, be necessarily confined to the form that evil had theretofore taken. Time works changes, brings into existence new conditions and purposes. Therefore a principle to be vital must be capable of wider application than the mischief which gave it birth. This is particularly true of constitutional. They are not ephemeral enactment's, designed to meet passing occasions. . . . The future is their care and provision for events of good and bad tendencies of which no prophecy can be made. In the application of a constitution, therefore, our contemplation cannot be only of what has been but of what may be." *Olmstead*, 277 U.S. at 473 (Brandeis, J. dissenting)

[70] "The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." *Olmstead*, 277 U.S. at 474.

[71] "[I]t follows necessarily that the [Fourth] Amendment is violated by the officer's reading the paper without a physical seizure, without his even touching it. . . . The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They know that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone--the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed must be deemed a violation of the Fourth Amendment." *Olmstead*, 272 U.S. at 572.

Despite its eloquence, Brandeis' view of the Fourth Amendment was not embraced by the Court until forty years later with the announcement of its decision in *Katz v. United States*, 389 U.S. 347 (1967).[72] Charles Katz was convicted of placing bets during interstate telephone calls. At trial, over objection by Katz, the prosecution presented audio tapes/transcripts of telephone calls that Katz made from a telephone booth. The tapes were made through the use of a recording device that was placed outside of the phone booth.[73]

The Court determined that the tapes were made in violation of Mr. Katz's Fourth Amendment rights. In writing for the seven-member majority, Justice Stewart rejected the physical trespass requirement of *Olmstead* and, instead, focused on the interference with the defendant's expectations of privacy. The opinion chastised the parties for missing the purpose of the Fourth Amendment's protection by debating whether telephone booths are constitutionally protected spaces. In a clear rejection of the logical foundation of *Olmstead*, the court noted that "the Fourth Amendment protects people, not places."[74] The issue then is not whether a particular space, *per se*, falls within a zone of constitutional protection, but whether the defendant's conduct reflected an actual and reasonable desire to maintain the privacy of the communications at issue. [75]

---

[72] See, e.g., *Goldman v. United States*, 316 U.S. 129 (1942) (holding that the use of a "detectaphone" listening device placed against the outer wall of an office did not implicate the Fourth Amendment because it did not involve a physical trespass.)

[73] *Katz*, 389 U.S. at 348.

[74] *Katz*, 389 U.S. at 351.

[75] "Because of the misleading way the issues have been formulated, the parties have attached great significance to the characterization of the telephone booth from which the petitioner placed his calls. The petitioner has strenuously argued that the booth was a 'constitutionally protected area.' The Government has maintained with equal vigor that it was not. But this effort to decide

It was Justice Harlan's concurring opinion, not the opinion of the majority, which provided the basic analytical framework that is still used to determine whether governmental action has violated the Fourth Amendment.[76] According to Justice Harlan, the location of the person, or the object searched, is essential to resolving most questions regarding the nature of the Fourth Amendment's right to be free from unreasonable intrusions. Justice Harlan articulated a two-part test, based on the Court's prior decisions, for determining whether the Fourth Amendment applies in a given factual context. First, the person invoking the right must have exhibited an actual expectation of privacy. Second, the expectation must be one that society is willing to recognize as reasonable.[77]

---

whether or not a given 'area,' viewed in the abstract, is 'constitutionally protected' deflects attention from the problem presented by this case. For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. See *Lewis v. United States*, 385 U.S. 206, 210; *United States v. Lee*, 274 U.S. 559, 563. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. See *Rios v. United States*, 364 U.S. 253; *Ex parte Jackson*, 96 U.S. 727, 733." *Katz*, 389 U.S. at 351.

[76] "Based on Justice Harlan's concurring opinion in *Katz v. United States*, the Supreme Court has developed a two-part test to determine whether a given inspection is a search: if the government action has violated an individual's subjective expectation of privacy, and if society recognizes that expectation as reasonable, then the inspection is a search and the protections of the Fourth Amendment apply. . . . [T]he *Katz* test remains the relevant inquiry for determining whether a search has taken place. *See California v. Caraolo*, 476 U.S. 207, 211 (1986)" *Note: Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 Harv. L. Rev. 1591, 1596 (May, 1997)

[77] "I join the opinion of the Court, which I read to hold only (a) that an enclosed telephone booth is an area where, like a home, *Weeks v. United States*, 232 U.S. 383, and unlike a field, *Hester v. United States*, 265 U.S. 57, a person has a constitutionally protected reasonable expectation of privacy; (b) that electronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment; and (c) that the invasion of a constitutionally protected area by federal authorities is, as the Court has long held, presumptively unreasonable in the absence of a search warrant.

"As the Court's opinion states, 'the Fourth Amendment protects people, not places.' The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a 'place.' My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is

Because the test incorporates an objective standard of contextual reasonability, the courts has been able to apply this method of analysis in a variety of factual settings.[78]

2. Fourth Amendment Doctrine Applied to Computers or Analogous Contexts

Is there a reasonable expectation of privacy in a computer? If only the issue were so straightforward. As a general proposition, computers are "repositories of personal information" such as financial records, personal notes, trade secrets, or visual images, and, as such, are deserving of protection via the Fourth Amendment.[79] However, Fourth Amendment doctrine requires us to consider the specific context of a search to determine whether the protections afforded by the Amendment are applicable. In undertaking this analysis, commentators and the few courts to address the issue, have applied analogical

---

prepared to recognize as 'reasonable.' Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable. *Cf. Hester v. United States, supra*." *Katz*, 389 U.S. at 361. (Harlan, J. concurring.)

[78] The Court has applied the two-part Katz test and determined that the following were not searches within the meaning of the Fourth Amendment: "examining trash left at the curb side for pickup, sniffing of luggage or automobile by detection dogs, employing a pen register, monitoring vehicles on the road by means of a beeper, placing beepers in containers outside of the home or curtilage, subpoenaing bank records, using undercover agents, flying over residential property, searching destroyed property, and examining magazines in a bookstore. [citations omitted.]" Francis A. Gilligan and Edward J. Imwinklereid, Cyberspace: The Newest Challenge for Traditional Legal Doctrine, 24 Rutgers Computer & Tech. L.J. 305, 326 (1998)

[79] Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 Harv. J.L. & Tech. 75, 81 (1994).

reasoning in resolving the issue.[80] Of course, the choice of analogy may be critical to the outcome.

A common analogy, particularly when evaluating the privacy interest in e-mail, is first class mail.[81] Courts have recognized a reasonable expectation of privacy in the contents of a sealed letter in the course of being forwarded by first class mail.[82] However, a message sent via e-mail is not sent to the recipient's computer in the same way that a first class letter is sent to the addressee. The message is sent to the computer of the e-mail service provider, which then sends a notification of an incoming message to the recipient's account. When the recipient, or someone with access to the account, forwards a command to read the message, a copy of the message is forwarded to the addressee's computer. Moreover, particularly in business and governmental settings, a network may be designed so that the network administrator automatically receives copies of all incoming and outgoing messages. Given the significant number of identical copies of the message which are accessible to people other than the addressee, among other differences, there is reason to question whether the analogy provides a sound basis for making legal conclusions.[83]

---

[80] The use of analogical reasoning to determine the applicability is not unique to computer-related searches. See, e.g., *United States v. Myers*, 46 F.3d 668, 670 (7th Cir.) cert. denied, 116 S.Ct. 213 (1995) (holding that the use of a thermal imager to detect heat emanating from a home did not constitute a search on the basis that it was comparable to a dog sniffing a luggage for drugs)

[81] See, e.g., Chris J. Katopsis, "Searching" Cyberspace: The Fourth Amendment and Electronic Mail, 14 Temp. Envtl. L. & Tech. J. 175, 176 (1995); Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 Harv. J.L. & Tech. 75, 81-82 (1994).

[82] *United States v. Maxwell*, 45 M.J. 406, 416 (C.A.A.F. 1996)

[83] It is worth noting that any expectation of privacy only exists while the message is in transit. Once the message is received, the sender generally loses any control over further dissemination. Just as with normal correspondence, "[w]hen an individual reveals private information to another,

Another common analogy involves the telephone. Assuming that the computer is connected to the Internet, or any other external source via a phone line, the analogy is quite apt. If voice communication over a particular phone line is deserving of privacy protection, transmission of data over the same line should probably also receive the same protection.

Yet, notwithstanding *Katz*, not all communication over a telephone has been held to deserve Fourth Amendment protection. In *Smith v. Maryland*[84], the Court held that the use of a pen register[85] by a telephone company to record the numbers dialed from a residential phone did not violate any reasonable expectations of privacy. The Court found that there were many legitimate business reasons why telephone companies may need to record such information[86]

However, recording numbers is not the same as recording the substantive content of the communication itself. Although Internet service providers may have a reason to monitor Internet addresses or e-mail destinations, they do not have any legitimate reason to monitor the content of the messages.

A third analogy is to consider "cyberspace" as a physical location or object. For instance, memory space on a computer could be analogized to a closed container or a file cabinet for purposes of evaluating the applicability of the

---

he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of the now nonprivate information . . . ." *United States v. Jacobsen*, 466 U.S. 109, 117 (1984)

[84] 442 U.S. 735 (1979)

Fourth Amendment.[87] In doing so, it is imperative to understand the quantity of information that can be held by an average personal computer. "A typical home computer with a modest 100 megabyte storage capacity can contain the equivalent of more than 100,000 typewritten pages of information."[88] The large capacity of a computer would seem to make comparisons to a filing system more apt than a single cabinet, especially when evaluating whether the warrant, if one was issued, satisfies the particularity requirement of the warrant clause. The container analogy is flexible enough to accommodate the fact that the actual computer in which records may be stored may be physically separate from the computer work station on which the owner/operator actually inputs/accesses the information;[89] the fact that the operator may not own the storage device being searched;[90] and that the search itself does not necessarily require any physical intrusion.[91]

Applying one or more of these analogies, courts have uniformly determined that information residing on a computer memory device is generally

---

[85] "Pen registers are used to identify outgoing numbers called from a subject's phone line." Legal Guide to Computer Crime, Office of the Staff Judge Advocate, Air Force Office of Special Investigations, (1994) at page 15.
[86] *Smith v. Maryland*, 442 U.S. at 743-44.
[87] Winick, 8 Harv. J. Law & Tech at 82
[88] *Id.* at 81.
[89] Courts have generally held that an expectation of privacy is not limited to objects within a home. See, *O'Connor v. Ortega*, 480 U.S. 707,718 (1987) (office), *United States v. Salinas-Cano*, 959 F.2d 861, 864 (10th Cir. 1992) (luggage), and *United States v. Bosby*, 675 F.2d 1174, 1180 (11th Cir. 1982).
[90] *Minnesota v. Olson*, 495 U.S. 91, 95-100 (1990), (overnight guest has reasonable expectation of privacy)
[91] *Katz*, 389 U.S. at 352 (1967).

entitled to the protections afforded by the Fourth Amendment.[92] This conclusion does not mean that a warrantless search of the information in a computer is necessarily unreasonable. The courts have recognized several exceptions, as noted above, to the basic notion that warrantless searches are not constitutional. The following section of the paper discusses the exception that appears most relevant to the activities that the Air Force might undertake in response to an unauthorized intrusion into the DII.

3. Exceptions to the Warrant Requirement

Notwithstanding the general doctrinal preference for warrants[93], it is clear that the Court is willing to recognize a number of situations in which the failure to obtain a warrant, or even the lack of probable cause, will not render a search unreasonable.[94] The following situations are among those in which the lack of a warrant will not necessarily invalidate a search: searches incident to a lawful arrest[95]; seizure of items in plain view[96]; exigent circumstances[97]; consent

---

[92] See, e.g., *United States v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996) (determining that a reasonable expectation of privacy existed in the private America Online account of an active duty Air Force officer charged with, among other things, transporting or receiving child pornography in interstate commerce.) ; *United States v. Lyons*, 992 F.2d 1029 (10th Cir. 1993) (seizure of data from hard disks did not violate defendant's subjective expectation of privacy because he had no right to exclude others from the property in question.); *United States v. Charbonneau*, 979 F.Supp. 1177 (S.D. Ohio 1997) (determining that the extent of the expectation of privacy in e-mail transmissions are contextually dependent.)

[93] *See Almeida-Sanchez v. United States*, 413 U.S. 266, 277 (1973) (Powell, J. concurring) ("But it is by now axiomatic that the Fourth Amendment's proscription of 'unreasonable searches and seizures' is to be read in conjunction with its command that 'no Warrants shall issue, but upon probable cause.'"); Johnson v. United States, 333 U.S. 10, 14 (holding that the requirement for a warrant exists absent an applicable pre-existing exception.)

[94] See, e.g., Jeremy J. Calsyn et al. Warrantless Searches and Seizures, 86 Geo. L.J. 1214 (1998)

[95] *United States v. Robinson*, 414 U.S. 218, 234-36 (1973) (The safety of the arresting officer justifies, but limits the scope of, a warrantless search of a person incident to a lawful arrest.)

[96] *Horton v. California*, 496 U.S. 128, 136 (1990) (No warrant required when officer is in a lawful position to observe apparently incriminating evidence.)

searches[98]; and border searches[99]. Although each exception stands on its own logical foundation, the general basis for the exceptions are that the "requirement" to obtain a warrant would frustrate an important governmental interest, such as ensuring the safety of the police, or the community, or the likely loss of evidence, which, under certain circumstances, outweighs the individual's interest in privacy.[100] Moreover, courts are more willing to permit a warrantless search when the search was conducted for some reason other than to obtain evidence of criminal misconduct.[101]

As discussed above, the circumstances that concern us in this paper involve an attack against the NII/DII. One of the first steps taken in response by the Air Force, and other law enforcement and national security agencies, is trying to determine the source of the attack. This typically involves attempting to trace the attack back through the series of intermediate computers that were used to obtain access to the target and camouflage the identity of the attacker.[102] The fundamental issue is whether the national security interests that may be served

---

[97] *Mincey v. Arizona*, 437 U.S. 385, 392-93 (1978) (Reasonable belief that entry is in response to one in need of "immediate aid" permissible.)
[98] *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973) (No warrant required if a person with authority has consented.)
[99] *United States v. Ramsey*, 431 U.S. 606 (1977) (Warrant not required at the border to search individuals or items entering the country.)
[100] "Generally, only fear of imminent destruction of evidence, hot pursuit, immediate threats to the safety of the public or the officers, or other emergencies will be sufficient to justify a warrantless entry into an individual's home to make an arrest." Jeremy J. Calsyn, Warrantless Searches and Seizures, 86 Geo. L.J. 1214, 1228 (1998) citing *United States v. Wilson*, 36 F.3d 205, 209-10 (1st Cir. 1994); *Unites States v. Rico*, 51 F.3d 495, 504 (5th Cir. 1995).
[101] See, e.g., Silas J. Wasserstrom, The Court's Turn Toward a General Reasonableness Interpretation of the Fourth Amendment, 27 Am. Crim. L. Rev. 119, 128 (1989)
[102] Michael Vatis, Chief, National Infrastructure Protection Center, Prepared Statement to the Senate Committee on Judiciary, Subcommittee on Technology, Terrorism, and Government Information, Federal News Service, June 10, 1998, at page 3.

by efforts to identify the attackers are of such substantial societal importance so as to justify the application or creation of an exception to the warrant requirement.

The interests being furthered by such a search are similar, but not identical, to those typically encountered in a hot pursuit or exigent circumstances scenario. It is easy to conceive of the Air Force action in such a way so that the primary differences stem from the lack of physicality of a cyber search. That is, although the Air Force agents are not physically chasing the suspect, they are engaged in a concerted effort to determine the identity of the suspect before he destroys evidence or commits further misconduct.[103] However, the Air Force is not necessarily motivated by a desire to obtain evidence of a crime when it pursues the initiator of a cyber attack. For the Air Force to be involved, the primary motivator must relate to an issue of national security.[104] For this reason, the "special needs" exception presents a much more appealing basis for analyzing whether the courts should deviate from the traditional interpretation of the Fourth Amendment and simply engage in a balancing of interests.

The "special needs" exception to the warrant requirement was first articulated in *New Jersey v. T.L.O.*[105]. *T.L.O.* involved a warrantless search in a school setting. An assistant vice principal searched the purse of a student who

---

[103] See, e.g., *U.S. v. Santana*, 427 U.S. 38 (1976)
[104] This reflects the institutional roles and responsibility of the military services vis-a-vis other federal agencies, such as the FBI, that are tasked with carrying out domestic law enforcement. In fact, as will be discussed below, the Posse Comitatus Act, 18 U.S.C. § 1385, specifically limits the participation of the Air Force in domestic law enforcement.
[105] 469 U.S. 325 (1985)

had been observed smoking in a lavatory in violation of school rules. The search produced evidence that the student was involved in the use and distribution of marijuana. That evidence, along with her confession, was used in delinquency proceedings and as a basis for administrative action by the school. The student challenged the admissibility of the evidence. The U.S. Supreme Court held that the evidence was obtained and used in a constitutional manner.

Justice White's opinion for the Court reflected the substantial governmental interest in "maintaining an environment [in the schools] in which learning can take place."[106] The Court engaged in a balancing analysis to determine whether the state interest in "swift and informal disciplinary procedures" outweighed the student's privacy interest.[107] Ultimately, the Court concluded that, because the "burden of obtaining a warrant is likely to frustrate the purpose behind the search" the warrant requirement would not be strictly applicable in the school setting.[108]

It is Justice Blackmun's concurring opinion, however, that introduced the principle of special needs that has now defined this class of exceptions to the warrant requirement. Justice Blackmun criticized the majority for engaging in a balancing analysis without explicitly stating that balancing the competing interests, rather than strictly applying the warrant requirement, was justified only

---

[106] *T.L.O.*, 469 U.S. at 340.
[107] *Id.*
[108] *Id.*

in light of the circumstances which demonstrated a "special law enforcement need for greater flexibility."[109]

> The special need for an immediate response to behavior that threatens either the safety of schoolchildren and teachers or the educational process itself justifies the Court in excepting school searches from the warrant and probable cause requirement, and in applying a standard determined by balancing the relevant interests.[110]

Since deciding T.L.O., the Court has applied the doctrine of special needs five times. *O'Connor v. Ortega*[111] held that special needs existed in the context of an office setting when an employer conducts a search of an employee's office. The Court characterized as "substantial" the government's interest in maintaining an efficient and proper workplace.[112]

In *Griffin v. Wisconsin*[113] the Court upheld a state regulation that authorized probation officers to conduct a warrantless search of a probationer's residence based simply on a reasonable suspicion that the search would produce evidence of a probation violation.[114] The Court determined that the special need to preserve "the deterrent effect of the supervisory arrangement" inherent in probation justified the departure from the warrant requirement.[115]

---

[109] *T.L.O.*, 469 U.S. at 350. (Blackmun, J. concurring)
[110] *Id.*, at 350-51. (Blackmun, J. concurring)
[111] 480 U.S. 709 (1987).
[112] *O'Connor v. Ortega*, 480 U.S. at 720. "In our view, requiring an employer to obtain a warrant whenever the employer wished to enter an employee's office, desk, or file cabinets for a work-related purpose would seriously disrupt the routine conduct of business and would be unduly burdensome."
[113] 483 U.S. 868 (1987)
[114] *Griffin*, 483 U.S. at 873-74.
[115] *Id.* at 878.

Skinner v. Railway Labor Executives Association[116] involved a challenge to federal regulations which mandated drug and alcohol testing of railroad employees. The Court upheld the regulations. "The Government's interest in regulating the conduct of railroad employees to ensure safety, like its supervision of probationers or regulated industries, or its operation of a government office, school, or prison, 'likewise presents "special needs" beyond normal law enforcement that may justify departures from the usual warrant and probable cause requirements.'" quoting *Griffin v. Wisconsin*, 483 U.S. 868, 873-74 (1987).

National Treasury Employees Union et al. v. Von Raab[117] was decided the same day as *Skinner*. *Von Raab* involved a challenge to a requirement by the United States Customs Service that employees who sought transfer or promotion to certain sensitive jobs. The requirement was upheld after balancing the respective interests. The interest identified by the Court as justifying the suspicion-less searches arose from the governmental duty to provide for the security of the nation.[118]

---

[116] 489 U.S. 602 (1989)

[117] 489 U.S. 656 (1989)

[118] "The Customs Service is our Nation's first line of defense against one of the greatest problems affecting the health and welfare of our population. * * * It is readily apparent that the Government has a compelling interest in ensuring that front-line interdiction personnel are physically fit, and have unimpeachable integrity and judgment. Indeed, the Government's interest here is at least as important as its interest in searching traveler's entering the country. * * * While reasonable tests designed to elicit [information that bears on employee's fitness to perform their duties] doubtless infringe some privacy expectations, we do not believe these expectations outweigh the Governments' compelling interests in safety and in the integrity of our borders." *Von Raab*, 489 U.S. at 670-71

The most recent special needs case is *Vernonia School District 47J v. Acton*[119]. The Court upheld the constitutionality of a school district's policy requiring students who wished to participate in school sponsored sports to submit to urinalysis drug testing. The opinion explained that the balancing approach was particularly appropriate for determining the Fourth Amendment implications of non-traditional governmental conduct. The Court identified the Government's interest as "deterring drug use by our Nation's schoolchildren" and determined that the manner in which the policy at issue furthered this interest outweighed the manner in which the policy intruded upon the privacy expectations of schoolchildren.[120] "Taking into account all the factors we have considered above—the decreased expectation of privacy, the relative unobtrusiveness of the search, and the severity of the need met by the search—we conclude Vernonia's Policy is reasonable and hence constitutional."[121]

There is an argument to be made that actions taken by the Air Force to determine the perpetrator of an ongoing cyber attack against this Nation's information infrastructure involves "special needs beyond normal law enforcement." The interest in defending our critical infrastructures against an "electronic Pearl Harbor" is compelling.[122] Long ago, the Court recognized that

---

[119] 515 U.S. 646 (1995)
[120] *Acton*, 515 U.S. at 659.
[121] *Acton*, 515 U.S. at 663.
[122] "It is a mistake, however, to think that the phrase 'compelling state interest,' in the Fourth Amendment context, describes a fixed, minimum quantum of governmental concern, so that one can dispose of a case by answering in isolation the question: Is there a compelling state interest here? Rather, the phrase describes an interest that appears important enough to justify the particular search at hand, in light of other factors that show the search to be relatively intrusive upon a genuine expectation of privacy." *Acton*, 515 U.S. at 659.

"[t]o preserve its independence, and give security against foreign aggression and encroachment, is the highest duty of every nation, and to attain these ends nearly all other considerations are to be subordinated."[123] To the extent that there is clear and credible evidence of a cyber attack against vital national security interests, a focused response to such a threat arguably deserves an exception from the warrant requirement of the Fourth Amendment.

There is one small glitch in this argument. In 1972, the Supreme Court held that the power and authority to provide for national security reserved to the President by the Constitution does not override the warrant requirement of the Fourth Amendment. That case, *United States v. United States District Court for the Eastern District of Michigan*, 407 U.S. 297 (1972) (referred to as the "*Keith*" case) arose from a criminal prosecution of three individuals charged with various counts of conspiring to destroy, and/or destroying, governmental property.[124] During pretrial proceedings at the criminal trial, the government conceded the existence of information pertaining to the defendants that was obtained through electronic surveillance.[125] The government refused to release this information to the defendants. The Attorney General presented an affidavit stating that he, and not a federal magistrate or judge, "approved the wiretaps 'to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government.'"[126]

---

[123] *Chinese Exclusion Case*, 130 U.S. 581, 606 (1889)
[124] *Keith*, 407 U.S. at 299.
[125] *Id.*
[126] *Id.*

Information pertaining to the surveillance was filed in a sealed exhibit for in camera inspection by the District Court.[127]

The Government asserted that the surveillance was lawful notwithstanding the lack of a warrant in that it constituted "a reasonable exercise of the President's power (exercised through the Attorney General) to protect the national security."[128] Both the District Court and the Sixth Circuit disagreed.[129] The Supreme Court affirmed.[130]

The Court noted that warrantless electronic surveillance had been practiced and sanctioned "more or less continuously by various Presidents and Attorney Generals since July 1946."[131] Yet, this was a case of first impression. The Court framed the issues as follows:

> As the Fourth Amendment is not absolute in its terms, our task is to examine and balance the basic values at stake in this case: the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression. If the legitimate need of Government to safeguard domestic security requires the use of electronic surveillance, the question is whether the needs of citizens for privacy and free expression may not be better protected by requiring a

---

[127] *Id.*

[128] *Keith*, 407 U.S. at 301.

[129] 321 F.Supp. 1074 (E.D. Mich. 1971), 444 F.2d 6511 (1971).

[130] *Keith*, 407 U.S. at 324. The vote was 8-0, with Justice Rehnquist not participating. Six justices joined in the opinion for the Court.

[131] *Keith*, 407 U.S. at 310. "The use of warrantless electronic surveillance to gather intelligence in cases involving threats to the Nation's security can be traced back to 1940, when President Roosevelt instructed Attorney General Robert Jackson that he was authorized to approve wiretaps of persons suspected of subversive activities. In 1946, President Truman's approval of Attorney General Tom Clark's request for expanded wiretapping authority to extend to cases involving 'domestic security.' *** Attorneys General serving Presidents Eisenhower, Kennedy, Johnson, and Nixon continued the practice of employing warrantless electronic surveillance in their efforts to combat perceived threats to national security, both foreign and domestic." *Mitchell v. Forsyth*, 407 U.S. 511, 529 (1985).

> warrant before such surveillance is undertaken. We must also ask whether a warrant requirement would unduly frustrate the efforts of Government to protect itself from acts of subversion and overthrow directed against it.[132]

Despite framing the issue as a conflict between two imperatives, the Court's analysis reflects the traditional view of Fourth Amendment doctrine that warrantless searches are presumptively unconstitutional. "Some have argued that 'relevant test is not whether it is reasonable to procure a search warrant, but whether the search was reasonable,' *United States v. Rabinowitz*, 339 U.S. 56, 66 (1950). This view, however, overlooks the second clause of the Amendment. The warrant clause of the Fourth Amendment is not dead language."[133]

Applying this understanding of Fourth Amendment jurisprudence, the Court held that under the circumstances presented "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch."[134]

Although the Court acknowledged the established exceptions to the warrant requirement, it determined that placing wiretaps in furtherance of domestic security goals did not fit within any of the carefully delineated exceptions.[135] Moreover, the Court rejected the Government's invitation to

---

[132] *Keith*, 407 U.S. at 313.
[133] *Keith*, 407 U.S. at 315.
[134] *Keith*, 407 U.S. at 316.
[135] *Keith*, 407 U.S. at 318.

create a separate exemption, on the basis that the benefit to national security did not justify the risk to individual liberties.[136]

The *Keith* opinion reflects a judicial decision-making process that is not entirely pure in terms of intellectual honesty. The Court presents the issue as one requiring a balance between individual liberty and national security. However, when it determines that based on the facts before it the individual liberty interest prevails, it explains its decision in terms of a rigid jurisprudence (the warrant requirement) that rejects a balancing analysis. In *TLO* and its progeny, the Court has come to terms with the necessity of developing a jurisprudence that is consistent with the underlying analysis that the Court does and should perform when presented with a novel situation involving a tension between individual privacy and the good of the community.

The most recent of the special needs cases provides the following summation of the relevant doctrine:

> As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is "reasonableness." At least in a case such as this, where there was no clear practice, either approving or disapproving the type of search at issue, at the time the constitutional provision was enacted, whether a particular search meets the reasonableness standard is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests . . . . Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, this Court has said that reasonableness generally requires the

[136] *Keith*, 407 U.S. at 320.

> obtaining of a judicial warrant. . . . But a warrant is not required to establish the reasonableness of all government searches; and when a warrant is not required (and the Warrant Clause therefore not applicable), probable cause is not invariably required either.[137]

Although I don't profess any special insight into the understandings and aspirations of the men who wrote the Constitution, it is probably safe to say that the framers did not envision the possible harm to our national security that could be wrought through a cyber attack. The notion of a viable cyber threat to the nation's infrastructure stems from the technological, commercial, and cultural developments of the past ten years. Consequently, the analysis of the *Keith* opinion did not, could not, properly account for the nature and scope of this threat.

The argument that the Air Force should not be required to obtain a warrant prior to initiating a response to a cyber attack would go as follows: A governmental response to such an attack furthers interests that are different, and require more flexibility than those involved in the typical criminal investigation. Providing for the security of the nation against an actual or potential threat to our critical infrastructures is due much more weight than the governmental interest in regulating the conduct of railroad employees to ensure safety, supervising probationers or regulated industries, or operating a government office, school, or prison and, therefore, outweighs the intrusion associated with a search of a computer that was involved in the attack. For

---

[137] *Acton*, 515 U.S. at 652

these reasons, the argument would go, the privacy interest of individual citizens would be outweighed by a collective desire to maintain national security.

However, there are some problems with this argument. The warnings and indications of a cyber attack are not any different from a simple crime. It is only after we have decided to undertake responsive action that we might be able to distinguish between an attack and a crime. As a matter of policy, eliminating the role of judiciary in making this determination is problematic. Our system of government is based upon a distribution of power among the various branches. It is particularly important in the context of protecting individual rights that the judiciary must serve as a check on the power of the executive, however well intentioned. The participation of the judiciary does not necessarily guarantee that the balance between rights and responsibilities will be struck optimally.[138] Nonetheless, the involvement of some judicial authority (at least in a manner similar to that followed in the context of foreign intelligence discussed below) increases the likelihood that the process will afford proper consideration to both individual rights and constitutional responsibilities.

The Fourth Amendment, however, isn't the only source of law that speaks to this issue. There are several statutes that impose material restrictions. It is significant, however, that the source of the restrictions are statutory, rather than constitutional for the obvious reason that if Congress determines that it is in the

[138] See e.g., Korematsu v. United States, 323 U.S. 240 (1944)

national interest to revise these statutes, it is within the power of Congress to do so.

B. 18 U.S.C. § 1030, Fraud and related activity in connection with computers.

The Counterfeit Access Device and Computer Fraud and Abuse Act of 1986 (Computer Fraud and Abuse Act) was one of the first legislative initiatives at the federal level designed specifically to criminalize computer misconduct.[139] Prior to its enactment, federal crimes involving computers were addressed through the application of traditional criminal statutes or by applying the mail and wire fraud statutes (18 U.S.C. §§ 1341 and 1343).[140] The provisions of the Computer Fraud and Abuse Act, codified at section 1030 of Title 18, have been amended several times, most recently by the National Information Infrastructure Act of 1996.

The focus of the legislation in 1984 was to assure the security of information contained in computers owned or operated by the federal government.[141] It "prohibited unauthorized access to certain categories of

---

[139] The Computer Abuse Amendments Act of 1990, Senate Rept. 101-544 (1990) This paper only addresses the relevant federal laws. This is not to suggest that there has been an absence of activity in this area at the state level. "Legislatures in the 1980s enacted a remarkably broad redefinition of criminal laws pertaining to computer systems. At the beginning of the decade, only two states had laws dealing specifically with computer-related crimes; both had enacted legislation at the end of the 1970's. No federal statute existed. By the end of the 1980's, forty-eight states had adopted criminal statutes tailored to interests in computer systems, information and related materials. This rapid development was the result of a singular recognition that computer systems contain substantial value and significant vulnerability." R. Nimmer, The Law of Computer Technology, West Group, 1997, at page 12-9.

[140] *Id.*

[141] "The decision to pass a statute that limited federal intervention to certain specific situations reflected legislators' realization that the scope of the computer crime problem was not well known and that their actions might have unforeseen repercussions. Legislators considered and rejected broader bills that criminalized the use of a computer as a part of a scheme to defraud that affected interstate commerce, choosing instead to protect only the most vital federal

computers if the defendant realized monetary gain or obtained access to classified material."[142] In 1996, the scope of the law was expanded to prohibit "fraud using computers and the destruction or alteration of data in computers without authorization. The new offenses applied to "computers used by financial institutions or the federal government"[143] and any "computer which is used in interstate or foreign commerce or communications."[144]

Although there haven't been many reported opinions interpreting the various provisions of the legislation, it was the basis for the widely publicized prosecution of Robert Tappan Morris in 1990. Mr. Morris was found to have knowingly infected various educational and military computers with a "worm."[145]

In its current form, the statute prohibits, among other things, the following activity:[146]

---

interests that could be injured by computer users." Note, "The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem," 43 Vand. L. Rev. 453, 454 (1990)

[142] "The Computer Abuse Amendments of 1990," Senate Report 101-544 (1990)

[143] *Id.*

[144] 18 U.S.C. § 1030(e)(2)

[145] *United States v. Morris*, 928 F.2d 504 (2d. Cir. 1991). "In the colorful argot of computers, a 'worn' is a program that travels from one computer to another but does not attach itself to the operating system of the computer it 'infects.' It differs from a 'virus,' which is also a migrating program, but one that attaches itself to the operating system of any computer it enters and can infect any other computer that uses files from the infected computer." *Morris*, 928 F.2d. at 505, n.1. For other reported opinions, see *United States v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997) and *United States v. Sablan*, 92 F.3d 865 (9th Cir. 1996)

[146] The statute incorporates the following definitions:
Computer: "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device".
Protected Computer: "a computer exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution, or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or which is used in interstate or foreign commerce or communications".

- knowingly accessing a computer without authorization, or exceeding authorized access, and thereby obtaining sensitive information that could be used to the injury of the United States or the advantage of a foreign nation;[147]
- knowingly accessing a computer without authorization, or exceeding authorized access, and thereby obtaining specified financial information, information from any department or agency of the United States, or any computer involved in interstate or foreign communication;[148]
- intentionally obtaining unauthorized access to a federal government computer;[149]
- knowingly causing the transmission of a program, information, code or command and thereby intentionally causing damage to a protected computer.[150]

This law deters, and permits the punishment of, individuals who commit cyber attacks against the NII/DII. However, because "hacking-back" involves the same kind of activity, it also affects the ability of the Air Force to respond to such attacks. It is the provision of 18 U.S.C. § 1030(a)(2)(C) that prohibits obtaining information through the unauthorized access of any computer involved

---

The issue of authorization is not specifically defined by the statute and has not been developed in the limited case law.

[147] 18 U.S.C. § 1030(a)(1)
[148] 18 U.S.C. § 1030(a)(2)
[149] 18 U.S.C. § 1030(a)(3)
[150] 18 U.S.C. § 1030(a)(5)(A)

in interstate communication that concerns the Air Force. One of the characteristics of a cyber attack is the uncertainty of its source and scope. To resolve some basic questions about who the perpetrators are, and what they might be trying to accomplish, the Air Force would need to trace the attack back through the intermediary computers to locate the origin of attack.

> "[I]n most cyber attacks, the identity, location, and objective of the perpetrator are not immediately apparent. Nor is the scope of his attack--i.e., whether an intrusion is isolated or part of a broader pattern affecting numerous targets. This means it is often impossible to determine at the outset if an intrusion is an act of vandalism, organized crime, domestic or foreign terrorism, economic or traditional espionage, or some form of strategic military attack. The only way to determine the source, nature, and scope of the incident is to gather information from victim sites and intermediate sites such as Internet Service Providers and telecommunications carriers.[151]

Even assuming the proper resolution of all Fourth Amendment issues, if the Air Force attempts to "hack back" through the computers through which the cyber attack has passed in order to determine the source of the attack, it will be obtaining information, through the unauthorized access, of computers involved in interstate communication.

The statute does contain an exemption for law enforcement and intelligence activities. Section 1030(f) provides as follows:

> This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State,

---

[151] Michael A. Vatis, Director, National Infrastructure Protection Center, Statement for the Record to the Senate Armed Service Committee, Subcommittee on Emerging Threats and Capabilities, Federal Document Clearing House, March 16, 1999, at page 2.

> or a political subdivision of a State, or of an intelligence agency of the United States.

It is certainly arguable that the phrase "protective" includes defensive national security operations. However, there is no discussion of this section in the legislative history.[152] The lack of an explicit exemption for national security is indicative of how recently we have understood the potential for furthering national security objectives through cyber operations. Although it probably does not reflect a conscious choice to limit the authority of national security agencies to take the necessary steps to defend the national information infrastructure, a clarification of congressional purpose and intent would be helpful to both the executive branch and the judiciary to ensure compliance with this intent.

However, even absent any clarification, there are organizations within the Air Force that are clearly not subject to the restrictions of Section 1030. The Air Force Office of Special Investigations performs both law enforcement and counter-intelligence functions. In addition, the Air Intelligence Agency, as the name implies, performs an intelligence mission. As the Air Force Information Warfare Center is a part of the Air Intelligence Agency, most responsive Air Force cyber operations would be carried out by an agency that receives the benefit of the section (f) exemption.

C. 10 U.S.C. § 2511, Interception and disclosure of wire, oral, or electronic communications

---

[152] Senate Report No. 99-432 reprinted at 4 U.S. Code and Cong and Admin. News page 2479.

This statutory provision is commonly known as Title III or the Federal Wiretap Act. It was originally enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Title III was a legislative response to the Supreme Court's decision in *Katz.* Following the lead of the Court, Congress used Title III as a means of updating the Federal Communications Act of 1934 and providing meaningful guidelines for the use of wiretaps.[153]

Title III permitted the Government to seize the contents of wire communications but placed a number of restrictions on this authority. For instance, wiretaps could only be used for the investigation of specified crimes; they could be used after a probable cause determination and a showing that other investigative techniques would not work; that they would be used in such a way as to reduce the likelihood that innocent conversations would be intercepted; and that the subject of the wiretap would be given notice of the seizure after the investigation concluded.[154]

At the time of enactment, however, it only applied to voice communications, regardless of the method of transmission.[155] By the mid-1980's, Congress realized that the failure of the statute to account for such modern means of communication as e-mail justified another revision.

---

[153] Basil W. Mangano, The Communications Assistance For Law Enforcement Act and Protection of Cordless Telephone Communications: The Use of Technology as a Guide to Privacy, 44 Clev. St. L. Rev. 99, 104 (1996)
[154] James X. Dempsey, Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy, 8 Alb. L.J. Sci. & Tech. 65, 71 (1997) citing 18 U.S.C. §§ 2511, 2516, 2518.
[155] *Id.*

The cure for this ill was the Electronic Communications Privacy Act (ECPA).[156] By extending some of the protections afforded to voice communication to electronic communication,[157] Congress was trying to "reestablish the balance between privacy and law enforcement, which Congress found had been upset, to the detriment of privacy, by the development of communications and computer technology and changes in the structure of the telecommunications industry."[158]

However, not all aspects of the protections afforded to voice communication were extended to electronic communications. Specifically, rather than limiting the interception of electronic communications to a list of specified serious offenses, the ECPA permitted intercepts whenever the investigation involved a felony.[159] Moreover, the statute did not specify that evidence obtained in violation of its restrictions regarding the intercept of electronic

---

[156] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508. In addition to extending some of the previously existing protections regarding the interception of voice communications to electronic communications, the ECPA also made it unlawful to obtain or alter, without authorization, stored electronic or wire communication. This provision is codified at 18 U.S.C. § 2701, Unlawful access to stored communication.

[157] Electronic Communications was defined as: "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;" 18 U.S.C. § 2510 (a)(12)

[158] Dempsey, 8 Alb. L.J. Sci. & Tech. at 72.

[159] *Id.* at 74.

communications would not be admissible as evidence in a subsequent judicial proceeding.[160]

In its current form, the Federal Wiretap Act includes a number of provisions that are designed to clarify the authority of law enforcement and intelligence agencies to intercept wire and electronic communications. It specifically authorizes employees or agents of commercial electronic communications services to provide technical assistance to "persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined by section 101 of the Foreign Intelligence Surveillance Act."[161] However, one of two conditions must be satisfied as a prerequisite for such assistance. Either there must be a court order directing the assistance, or there must be a certification from the Attorney General, or other authorized governmental official, that "no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required."[162]

In the *Keith* opinion, although the Court held that the warrant requirement was applicable to electronic surveillance conducted in response to a domestic threat to national security, it also made clear that the same procedures established under Title III for ordinary law enforcement need not apply. "[W]e do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case. We recognize that domestic security

---

[160] *Id.* at 74.
[161] 18 U.S.C. § 2511(2)(a)(ii)

surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime.'"[163] Although the Court did not offer any specific guidance on the particular authorization procedures that might be acceptable within the national security context, it advised that "[d]ifferent standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[164]

Congress should accept the Court's invitation and establish authorization procedures for responses to computer intrusions determined to present a credible threat to critical infrastructures. At a minimum, Congress should amend the Federal Rules of Criminal Procedure so that Air Force officials are not required to obtain different search authorizations for each intermediate computer. In its current form Rule 41 requires a judicial official from the district within which the object is located to authorize the search. This requirement can quickly become an obstacle to an efficient national security/law enforcement response without providing any additional protection to individual liberties.

D. The Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act (FISA) was enacted in 1978 to regulate electronic surveillance in the national security context. It replaced the "national security disclaimer" that previously existed in the Federal Wiretap Act:

---

[162] *Id.*
[163] *Katz*, 407 U.S. at 321.
[164] *Id.*

> Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.[165]

Congress considered FISA a necessary response to the abuses of the intelligence gathering machinery that were permitted by the unchecked discretion afforded by the national security disclaimer.[166] Although many abuses came to light during the investigation into the Watergate break-in, Congressional inquiry revealed that the problem was not limited to a single presidency. Although the "number of illegal or improper national security taps and bugs conducted in the Nixon administration may have exceeded those in previous administrations", the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, chaired by Senator Frank Church, concluded that "every President since Franklin D. Roosevelt asserted the authority to authorize warrantless electronic surveillance and exercised that authority."[167]

Notwithstanding the abuses that had occurred, Congress recognized the necessity of carrying out electronic surveillance to gain intelligence data related

---

[165] 18 U.S.C. § 2511(3) (repealed 1978)

[166] "As I read it--and this is my fear--. . . the President . . . could declare--name your favorite poison--draft dodgers, Black Muslims, the Ku Klux Klan, or civil rights activists to be a clear and present danger to the structure or existence of the Government and thus possibly exempt from Title III's procedures under 2511(3)." 114 Cong. Rec. 14, 750 (1968) (remarks of Senator Hart).

to legitimate national security interests. FISA reflects the intent of Congress to put in place a "secure framework by which the Executive Branch could conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights."[168]

FISA establishes the United States Foreign Intelligence Surveillance Court (FISA court) comprised of seven federal district court judges appointed by the Chief Justice of the Supreme Court.[169] As a general matter, a warrant from one of the FISA court judges is a prerequisite to conducting electronic surveillance against a target that falls within the scope of FISA.[170]

FISA pertains to electronic surveillance of foreign powers or their agents, including "United States persons," conducted for the purpose of obtaining "information that relates to . . . the ability of the United States to protect against actual or potential attack or other grave hostile acts . . . ; sabotage or international terrorism by a foreign power or an agent of a foreign power; and, clandestine intelligence activities by an intelligence service or network of a foreign power. . . ."[171] Moreover, FISA requires the adoption of technical and

---

[167] Robert A. Dawson, Foreign Intelligence Surveillance Act: Shifting the Balance: the D.C. Circuit and the Foreign Intelligence Surveillance Act of 1978, 61 Geo. Wash. L. Rev. 1380, 1386 (June 1993)

[168] Id. at 1386. Quoting from Foreign Intelligence Surveillance Act of 1978: Hearing Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary, 95th Cong., 1st Sess. 13 (1977) reprinted in U.S.C.C.A.N. 3904.

[169] 50 U.S.C. § 1803(a)

[170] In certain circumstances, electronic surveillance may be conducted under the authority of the Attorney General rather than the FISA court. Among other things, the Attorney General must certify that the "surveillance is directed solely at communications used exclusively between or among foreign powers", and that there is "no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party." 50 U.S.C. § 1802(a)

[171] 50 U.S.C. § 1801(e)

administrative procedures designed "to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons. . . ."[172]

FISA essentially incorporates Title III jurisprudence by requiring an order the FISA court whenever a warrant would be required for law enforcement purposes.[173] However, there are significant differences between procedural aspects of the FISA regime and that of the Fourth Amendment/Title III. For instance, under Title III, a magistrate must find that there is credible evidence that the search will produce evidence of a specific criminal violation. Under FISA, surveillance may be conducted upon a showing of probable cause that the subject's activities may involve criminal activity.[174] Additionally, there is no requirement for the subject of a legally authorized FISA search ever to be notified that the search was conducted or to review the information that was obtained.[175] Notwithstanding these differences, FISA has withstood every legal challenge to its facial validity.[176] "Although the Supreme Court has never considered whether the balance struck by FISA is constitutional, FISA has survived numerous constitutional challenges in the lower courts. The view expressed by the Second Circuit . . . is representative: "We regard the

---

[172] 50 U.S.C. § 1801(h)
[173] 50 U.S.C. § 1801(f)
[174] 50 U.S.C. § 1801(b)(2)
[175] 50 U.S.C. § 1806(f)
[176] See Americo R. Cinquegrana, The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978: 137 U. Pa. L. Rev. 793, 816-17 (1989) Even prior to the passage of FISA, "virtually every court that addressed the issue had concluded that such surveillances constituted an exception to the warrant requirement of the Fourth Amendment." *United States v. Duggan*, 743 F.2d 59 (2nd Cir. 1984)

procedures fashioned in FISA as a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information."[177]

FISA was not drafted with cyber searches in mind. One of the classic traits of a cyber intrusion is the indirect path that the intruder follows before reaching the target computer. Quite often, the path goes through several computers in the United States. Consequently, in FISA terminology, the search would be of a United States person.[178]

FISA affords additional protections to United States persons. To conduct a search of such an entity under FISA, the Air Force would be required to demonstrate that the United States person was knowingly involved, on behalf of a foreign power, in various activities that are adverse to the national security interests of the United States. It is typically not possible to make this showing as any "assistance" given to the attacker by the owner of the computer was completely passive. It is unlikely that the owner of the computer was even aware of the intrusion into its system, particularly in a way that could give rise to a showing of potential culpability. Consequently, the procedures established by FISA are of marginal relevance in initially responding to cyber attacks that pass through computers belonging to legitimate entities within the United States. The

---

[177] Dawson, 61 Geo. Wash. L. Rev. 1380, 1395 (June 1993)

[178] "'United States person' means a citizen of the United States, an alien lawfully admitted for permanent residence . . ., an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States. . . ." 50 U.S.C. § 1801(i)

ultimate answer seems to require a hybrid between FISA and the Federal Wiretap Act that exclusively addresses the cyber threat.

E. The Posse Comitatus Act[179]

The Posse Comitatus Act (18 U.S.C. § 1385) reflects the deeply rooted belief in American political culture that the military should be subordinate and subservient to a strong civil authority.[180] This tradition of limiting the role of the military in domestic civil matters has had a place in Anglo-American law since the promulgation of the Magna Carta in 1215.[181] The PCA was enacted in 1878 in response to Southern anger over the use of soldiers in civilian law enforcement

---

[179] Posse Comitatus means: "The power or force of the county. The entire population of a county above the age of fifteen, which a sheriff may summon to his assistance in certain cases, as to aid him in keeping the peace, in pursuing and arresting felons, etc." Black's Law Dictionary 1162 (6th ed. 1990). This phrase derives from the Roman practice of permitting retainers to accompany and protect government official's enroute to their places of duty. This practice was known as "comitatus." See also, Furman, 7 Mil. L. Rev. 85, 87 (1960)

[180] "Whenever you conclude that it is right to use the Army to . . . discharge those duties that belong to civil officers, and to the citizens, then you have given up the character of your Government; it is no longer a government for liberty; . . . it has become a government of force." 7 Cong. Rec. 4247 (1878) (statement of Senator Hill) quoted in Fourth Amendment and Posse Comitatus Act Restrictions on Military Involvement in Civil Law Enforcement, 54 Geo. Wash. L. Rev. 404, 404 n.4, (1986). See also *Laird v. Tatum*, 408 U.S. 1, 15-16, 33 L. Ed. 2d 154, 92 S. Ct. 2318 (1972),:

> The concerns of the Executive and Legislative Branches . . . reflect a traditional and strong resistance of Americans to any military intrusion into civilian affairs. That tradition has deep roots in our history and found early expression, for example, in the Third Amendment's explicit prohibition against quartering soldiers in private homes without consent and in the constitutional provisions for civilian control of the military. Those prohibitions are not directly presented by this case, but their philosophical underpinnings explain our traditional insistence on limitations on military operations in peacetime. Indeed, when presented with claims of judicially cognizable injury resulting from military intrusion into the civilian sector, federal courts are fully empowered to consider claims of those asserting such injury; there is nothing in our Nation's history or in this Court's decided cases, including our holding today, that can properly be seen as giving any indication that actual or threatened injury by reason of unlawful activities of the military would go unnoticed or unremedied.

[181] Roger Blake Hohnsbeen, Fourth Amendment and Posse Comitatus Act Restrictions on Military Involvement in Civil Law Enforcement, 54 Geo. Wash. L. Rev. 404, 404 (1986)

roles following the Civil War to support the Reconstruction governments installed in the South.[182]

The PCA provides as follows:

> Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.[183]

Attorney General Reno recently testified to a congressional oversight committee about her understanding of the PCA.[184] It is her view that the limitations of the PCA are purely statutory and that Congress has the authority to

---

[182] Testimony of Brigadier General Walter B. Huffman, Assistant Judge Advocate General of Military Law and Operations, United States Army, before the House Judiciary Committee, July 20, 1995. See, e.g., Harold Human, Ulysses Grant I, Emperor of America?: Some Civil-Military Continuities and Strains of the Civil War and Reconstruction, in The United States Military Under the Constitution of the United States, (Richard H. Kohn ed., 1991):

[The Military Reconstruction Laws] one way or another imposed on the Army the duties of initiating and implementing state-making on the basis of biracial citizen participation. Protecting the personnel of the federal courts and Freedman's Bureau, shielding blacks and whites who collaborated in the new order of equality under state law from retaliations by indignant vigilante neighbors, and monitoring the quality of the daily marketplace justice in ten thousand villages--these were tasks that West Point had not prepared Army officers to perform.

[183] 18 U.S.C. § 1385 (1998) Currently, the maximum fine for individuals is $250,000. See 18 U.S.C. § 3571(b) Although the PCA does not explicitly apply to the Navy, the Department of Defense imposes its limitations on the Navy as a matter of executive policy. See Department of Defense Directive Number 5525.5, DoD Cooperation with Civilian Law Enforcement Officials (January 15, 1986)

[184] "The 'posse comitatus' restriction on the use of U.S. military forces to enforce laws within the United States is not contained in the Constitution but rather in a post-reconstruction era Act of Congress. See 18 U.S.C. § 1385. That Act expressly recognizes that Congress can enact statutes authorizing military involvement in law enforcement. Further, its provisions have been construed by the courts to be limited to activities that involve the direct execution of laws, e.g., making arrests. In contrast, the Posse Comitatus Act has not been construed to preclude the military from providing logistical, technical, and other forms of assistance to law enforcement. For example, the military has traditionally provided assistance to law enforcement in explosive ordnance disposal. [Recently,] Congress enacted statutes specifically addressing the use of the military in response to terrorist incidents involving chemical and biological weapons of mass destruction. 10 U.S.C. § 382; 18 U.S.C. §§ 175a and 2332e. Further, more generic statutes

authorize military involvement in law enforcement activities. This authority has been used, among other things, to authorize military assistance of drug interdiction operations.[185]

The remainder of this section examines the manner in which courts have interpreted the PCA; recent amendments to the PCA; and the implications of the PCA to efforts by the Air Force to respond to a cyber attack.

1. Judicial Interpretation

The PCA is a criminal statute. Yet, it the 120 years that it has been in effect, no one has ever been prosecuted for violating its terms.[186] Courts have had the opportunity to apply and interpret it in only a few instances. The majority of these have involved efforts by criminal defendants who argued that their prosecution was unlawfully assisted by the efforts of military personnel in violation of the PCA.[187] Others involved the use the PCA as a basis for a private cause of action against the military officials who authorized or participated in a particular operation.[188] Finally, there has been one case in which the United

---

authorize the President to use military forces to resolve domestic emergencies. 10 U.S.C. §§ 331-333.

[185] Defense Drug Interdiction Assistance Act, Pub. L. No. 99-570, §§ 3051-57 (1986)

[186] Matthew Carlton Hammond, The Posse Comitatus Act: A Principle in Need of Renewal, 75 Wash. U. L. Q. 953, 961 (Summer 1997) citing Posse Comitatus Act: Hearing Before the Subcomm. on Crime of the Comm. on the Judiciary on H.R. 3519, 97th Cong., 1st Sess. 10-11 (1981) (statement of Edward S.G. Dennis Jr., Chief, Narcotics and Dangerous Drug Sec., Criminal Division, U.S. Department of Justice) and Peter M. Sanchez, The "Drug War": The U.S. Military and National Security, 34 A.F. L. Rev. 109, 117 (1991).

[187] See, e.g., *United States v. Walden*, 490 F.2d 372, 375 (4th Cir.) cert. denied, 416 U.S. 983 (1974); *United States v. Cotten*, 471 F.2d 744, 747-48 (9th Cir.) cert. denied, 411 U.S. 936 (1973); *United States v. Casper*, 541 F.2d 1275 (8th Cir. 1976), cert. denied, 430 U.S. 970 (1977); *Gilbert v. United States*, 165 F.3d 470 (6th Cir. 1999).

[188] *Bissonette v. Haig*, 776 F.2d 1384 (8th Cir.1985); aff'd en banc, 800 F.2d 812 (8th Cir.1986), aff'd, 485 U.S. 264, 108 S. Ct. 1253, 99 L. Ed. 2d 288 (1988).

States used the PCA to shield itself from liability in an action brought under the Federal Tort Claims Act.[189]

Some aspects of the PCA have received a uniform interpretation and application by the courts. For instance, notwithstanding the many general references by the framers[190] to limitations on military involvement in domestic civil affairs, the courts have understood the specific limits imposed by the PCA as within the power of the Congress to modify or except.[191] However, the courts have been less than successful in providing a single meaningful test for determining what constitutes use of Army or Air Force personnel as a "posse comitatus."

Generally, courts have applied one or all of the following tests to determine whether the PCA has been violated:

---

[189] *Wrynn v. United States*, 200 F.Supp. 457 (E.D.N.Y. 1961)

[190] "The framers of the Constitution were determined to limit the military's role in civilian life after experiencing the unpopular use of British troops to maintain order in the American colonies during the decade prior to independence. An intense distrust of standing armies permeated the former colonist's lives and found expression in a number of contemporary political writings. . . . The Constitution reflects a general concern about potential dangers associated with a standing army. The document creates a scheme in which the armed forces must answer to a civilian commander in chief [U.S. Const. art II, § 2, cl. 1.]; Congress possesses exclusive control over key factors relating to the military's maintenance and use [art I, § 8, cls. 11, 12, 14]; the population at large may bear arms [amend. II]; troops may not be quartered in civilian homes in time of peace [amend III] . . . and the militia alone is expressly empowered to assist in enforcing the laws of the nation [art. I, § 8, cls. 15]. Moreover, in urging ratification of the Constitution, one of its principal authors, Alexander Hamilton, stressed the document's capacity to keep the nation's military forces from playing a deleterious role in the day-to-day operation of peacetime civil society." Christopher A. Abel, Not Fit for Sea Duty: The Posse Comitatus Act, the United States Navy, and Federal Law Enforcement at Sea, 31 Wm. and Mary L. Rev. 445, 449-50 (Winter, 1990)

[191] The purpose of this Act is to uphold the American tradition of restricting military intrusions into civilian affairs, except where Congress has recognized a special need for military assistance in law enforcement. *United States v. Walden*, 490 F.2d 372, 375 (4th Cir.), cert. denied, 416 U.S. 983 (1974) But see 7 Cong. Rec. 4240, 4243 for the proposition that several Senators understood the PCA to be nothing other than an expression of existing constitutional limitations on the use of military force.

(a) Direct, active involvement of one or more military personnel. A particularly lucid explanation of this test is found in *United States v. Red Feather*, 392 F.Supp. 916 (1974). The opinion notes that "the prevention of the use of military supplies and equipment was never mentioned in the debates, nor can it reasonably be read into the words of the Act."[192]

(b) Use of one or more military personnel in such a manner that it pervades the activities of the civil law enforcement organizations.[193] Although this analysis would permit the use of equipment, it would preclude the use of military personnel to operate or maintain the equipment if the equipment had a material effect on the outcome of the operation. It would even preclude the use of military advisors, if their advice related to a significant aspect of the operation and was followed by the civil authorities:

> If there was "use" of "any part of the Army or the Air Force" to "execute the laws" and if that use pervaded the activities of the United States marshals and the Federal Bureau of Investigation agents, the marshals and the agents cannot be said to have been "lawfully engaged" in the "lawful performance" of their official duties.[194]

---

[192] *Red Feather*, 392 F.Supp. at 922. "Of primary concern was the prospect of United States marshals, on their own initiative, calling upon troops to form a posse or to otherwise perform direct law enforcement functions to execute the law. 7 Cong. Rec. 3579-86, 3846-49. Thus, Representative Knott, the House sponsor of the legislation, stated as explanation that the act was intended to stop army troops, whether one or many, from answering the call of any marshal or deputy marshal to perform direct law enforcement duties to aid in execution of the law. 7 Cong. Rec. 3849. Se also, Id. at 4241. (remarks of Sen. Beck.) The appropriations restriction for fiscal year 1879 was therefore directed specifically to the 'employment of any troops in violation of this section.'" See also *Chandler v. United States*, 171 F.2d 921 (1st Cir. 1948) and *Gillars v. United States*, 182 F.2d 962 (1950).

[193] This analysis was developed in *United States v. Jarmillo*, 380 F.Supp 1375 (D.Neb. 1974).

[194] *Jaramillo*, 380 F.Supp. at 1379.

(c) Use of military personnel in a manner that constitutes the exercise of regulatory, proscriptive, or compulsory military power.[195] The focus of this test is on the manner in which military power is brought to bear against the citizenry:

> It is the nature of their primary mission that military personnel must be trained to operate under circumstances where the protection of constitutional freedoms cannot receive the consideration needed in order to assure their preservation. The posse comitatus statute is intended to meet that danger. [T]he feared use [of military personnel] which is prohibited by the posse comitatus statute is that which is regulatory, proscriptive or compulsory in nature, and causes the citizens to be presently or prospectively subject to regulations, proscriptions, or compulsions imposed by military authority.[196]

2. Implications for Air Force Information Infrastructure Defense Operations

It is generally accepted that, regardless of the correct test for determining the meaning of "posse comitatus," the use of military personnel to execute an arrest, or to search or seize evidence is prohibited by the PCA. This proscription is considered not applicable when the alleged perpetrator is a military member or the crime was directed at military assets.[197] As discussed above, cyber attacks are almost always indirect. Consequently, the initial steps taken by military investigators to track down the infiltrator will involve the search of computer

---

[195] See *United States v. McArthur*, 419 F.Supp. 186 (D. N.Dak 1975) *aff'd sub nom United States v. Casper*, 541 F.2d 1275 (8th Cir. 1976)
[196] *MacArthur*, 419 F.Supp. 193-94.
[197] *United States v. Banks*, 539 F.2d 14, cert. denied 429 U.S. 1024 (1976)

assets of innocent entities whose computer resources were used to carry out the attack. Searches and seizures of private computer resources during an initial response to a cyber attack or intrusion into critical aspects of the NII may amount to a search or involve a seizure of evidence. These actions are sufficiently direct and proscriptive that they should be deemed as falling within the scope of the PCA. Consequently, without any specific statutory exception, the PCA presents a serious limitation on the ability of the Air Force to respond.

The statutory exceptions necessary to remove conduct from the proscriptions of the PCA need not be part of the PCA. For instance, in the cases arising out of the involvement of Army personnel and equipment in response to the uprising by members of the American Indian Movement at Wounded Knee, South Dakota in 1973, the courts considered the Economy Act of 1932, 31 U.S.C. § 686, as creating a possible exception. This enactment provided executive branch departments with the authority to request and provide a variety of forms of assistance to each other.[198] To the extent that the conduct at issue was authorized by the Economy Act, the PCA was not offended.

Recently, Congress has expressed its view that military personnel and resources may be used in settings that implicate the traditional responsibilities of law enforcement organizations as well the national security function of the armed forces. Specifically, Congress has authorized the use of military assets, within specified parameters, to assist law enforcement organizations in accomplishing

---

[198] *Red Feather*, 392 F.Supp at 923.

their counter-narcotics activities, and in training for and responding to terrorist activities involving chemical and biological weapons.[199]

A similar statutory authorization is necessary to permit military personnel to assist in responding to cyber attacks against the NII.

F. International Law: Use of Force/Unlawful Aggression

To this point, the paper has considered domestic legal limitations on the ability of the United States Air Force to defend this nation's NII against a cyber attack. This section identifies and analyzes one category of limitations that are rooted in the law of nations.

The question that this section seeks to answer is the following: What are the international law implications of a computer network intrusion? For instance, what are the implications when the Air Force accesses without authorization a computer that is physically located in the territory of another sovereign at a time when the United States and the other sovereign are not in a state of belligerency? In the language of international law, does such an act constitute an unlawful use of force, unlawful aggression, or an impermissible intervention into the sovereignty of the other state?

The first step in addressing the question, of course, is to set out the applicable legal doctrine. As customary international law is not static, I'll discuss not only the current state of the pertinent law, but provide a brief description of its evolution. Next, I will outline three factual scenarios involving slightly different

[199] See 10 U.S.C. § §370-382

contexts in which the foreign computer is accessed. Finally, I will apply the law to the different scenarios.

1. International Law Regarding the Use of Force

(a) General Principles of International Law

There are two primary sources of international law: (1) international agreements and, (2) customary international law.[200] An international agreement is any binding commitment among nations, states or other legal entities regardless of whether it is characterized as a treaty, convention, protocol etc.[201]

Customary international law itself has two primary components: "(1) patterns of practice or behavior, and (2) patterns of legal expectation, 'acceptance' as law, or *opinio juris*."[202] Although technically only binding on signatories, international agreements can become binding on all international legal entities as customary international law if the predominant view of responsible and influential nations is that the terms of the agreement reflect the law of the international community and that these nations, in fact, adhere to these terms.[203]

---

[200] Jordan Paust et al., International Criminal Law, Cases and Materials, pages 3-4. (1996)
[201] *Id.* at 4.
[202] Jordan Paust, *International Law as Law of the United States*, at 1. (1995)
[203] "The customary international law of armed conflict derives from the practice of military and naval forces in the field, at sea, and in the air during hostilities. When such a practice attains a degree of regularity and is accompanied by the general conviction among nations that behavior in conformity with that practice is obligatory, it can be said to have become a rule of customary law binding upon all nations. It is frequently difficult to determine the precise point in time at which a usage or practice of warfare evolves into a customary rule of law. In a period marked by rapid developments in technology, coupled with the broadening spectrum of warfare to encompass insurgencies and state sponsored terrorism, it is not surprising that nations often disagree as to the precise content of an accepted practice of warfare and to its status as a rule of law." The United States Navy, *Annotated Supplement to the Commander's Handbook on the Law of Naval Operations*, pages 5-10. (1989)

(b) Historical Evolution of International Norms Regarding the Use of Force

The earliest legal doctrine regarding the use of force was premised on the concept of a "just war."[204] The doctrine, reflecting the Christianization of the Roman Empire, posited that "force could be used provided it complied with the divine will . . . . War was to be embarked upon to punish wrongs and restore the peaceful *status quo* but no further."[205]

The doctrine simply could not cope with the advent of wars between European Christian states, each of which was convinced that the divine will supported its particular cause.[206] Consequently, legal doctrine attempted to place limits on what were deemed acceptable justifications for the use of force as well as emphasizing efforts at peacefully resolving differences.[207] The doctrine of just war was redefined "in terms of self-defence, the protection of property and the punishment for wrongs suffered by the citizens of the particular state."[208]

"The period 1648 - 1815 is characterized by the relegation of the just war doctrine to the realms of morality or propaganda since in deference to public opinion governments frequently took pains to advance reasons for declaring war which would give the action some color of righteousness . . . ."[209] This same period witnessed the genesis of legal doctrine that reflected the power and

---

[204] Malcom Shaw, *International Law*, 539-41 (1986)
[205] *Id.*
[206] *Id.*
[207] *Id.*
[208] *Id.*
[209] Ian Brownlie, *International Law and the Use of Force by States*, 14-50 (1981) As excerpted in Barry Carter and Phillip Trimble, *International Law*, (1991)

authority of sovereign states to declare war whenever they deemed it to be in their national interest.[210] As states could not presume to judge another's cause, the law of neutrality "based on the assumption that the war was lawful on both sides" was developed.[211]

In the nineteenth century, war was looked upon as the "litigation of nations."[212] It was "a means of last resort after recourse to available means of peaceful settlement had failed."[213] State policies evolved in response. Lesser forms of coercion, such as reprisals or blockades, were developed. "The most important conclusion to be drawn from the nineteenth century experience is the unsatisfactory nature of 'war' as a term of art in view of the freedom which the concept conferred on states in characterizing their own actions."[214]

During the early twentieth century, there were several attempts to limit the acceptable uses of force by states. For instance, Article I of Hague Convention II reflects an agreement "not to have recourse to armed force for the recovery of contract debts claimed from the Government of one country by the Government of another country as being due to its nationals."[215] However, the prohibition was not applicable when efforts towards a peaceful resolution had failed.[216]

---

[210] *Id.*
[211] *Id.*
[212] *Id.*
[213] *Id.*
[214] *Id.*
[215] Convention Respecting the Limitation of the Employment of Force For the Recovery of Contract Debts, Signed at the Hague, October 18, 1907, 36 Stat. 2241, T.S. 537.
[216] *Id.*

The League of Nations was created after the First World War to "promote international co-operation and to achieve international peace and security."[217] "War, as such, was not made illegal but only where begun without complying with the requirements of the Covenant with regard to prior resort to pacific settlement of the dispute."[218] The enforcement mechanism was dependent upon the discretion of each state to implement any sanctions recommended by the Council of the League. "Apart from half-hearted economic sanctions against Italy in 1935, no sanctions were ever really applied by the League. To this extent the failure of the League was due, not to the inadequacies of the Covenant, but to the apathy and reluctance of the member states to discharge their obligations."[219]

In July 1929 the General Treaty for the Renunciation of War (commonly known as the Kellogg-Briand Pact) became effective. It solemnly declared on behalf of the signatories "that they condemn recourse to war for the solution of international controversies, and renounce it as an instrument of national policy in their relations with one another."[220] The agreement did not include an enforcement mechanism. The Second World War began ten years later. Nonetheless, as of January 1990, the Kellogg-Briand Pact remained in effect and had been ratified by 66 nations.[221]

---

[217] Bowett, *The Law of International Institutions*, pages 17-18, (1982). excerpted in Henkin et al., *International Law, Cases and Materials*, (1993)
[218] *Id.*
[219] *Id.*
[220] Article I, Kellog Briand Pact, August 27, 1928, 46 Stat. 2343, 94 L.N.T.S. 57.
[221] Carter and Trimble, *International Law*, page 1228 (1991)

(c) The Current Law

Although customary international law continues to reflect the principles discussed above, the most authoritative source of law regarding the use of force is the United Nations Charter.[222] Article 1(1) describes the principle purpose of the United Nations: "to maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to the breach of the peace . . . ."

The principle substantive legal norms prescribed by the Charter are contained in Articles 2(3) and 2(4). In addition, Article 51 limits the Charter's limitations on the authority of sovereign states to use force by acknowledging the "inherent right" of self-defense.

Article 2(3)

> All members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice are not endangered.

Article 2(4)

> All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any

[222] "The [UN] Charter remains the authoritative statement of the law on the use of force. It is the principal norm of international law of this century." L. Henkin, Use of Force: Law and U.S. Policy, *Right v. Might*, 37-69, (1989)

> state, or in any other manner inconsistent with the Purposes of the United Nations.
>
> Article 51
>
> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security . . . .

If anything is clear from these excerpts, it is that international law regarding the use of force is not without ambiguity.

Unlike the League of Nations Covenant and the Kellogg-Briand Pact, the term "war" is not used. "[I]t had become evident in the 1930's that States engaged in hostilities without declaring war or calling it war. The term 'force' was chosen as a more factual and wider word to embrace military action."[223] But the broader reach of the term force infuses ambiguity without necessarily limiting the ability of a state to circumvent it.

> The basic provision restricting the use of force (or its threat) in international relations is Article 2, paragraph 4, of the [UN] Charter. . . . The paragraph is complex in its structure and nearly all of its key terms raise questions of interpretation. We know that the principle was intended to outlaw war in its classic sense, that is, the use of military force to acquire territory or other benefits from another State. . . . The term "force" . . . has its own ambiguities. It is sometimes used in a wide sense to embrace all types of coercion: economic, political, and psychological as well as physical. Governments in the United Nations have from time to time sought to give the prohibition in Article 2(4) the wider meaning particularly to

[223] Schachter, *International Law in Theory and Practice*, 110-113 (1991), excerpted in Henkin et al., *International Law Cases and Materials*, (1993)

> include economic measures that were said to be coercive. Although support was expressed by a great many states in the Third World for this wider notion, it was strongly resisted by the Western States.[224]

Even assuming a satisfactory resolution of the scope of the term "force," a textual analysis of Article 2(4) raises issues as to the extent of the prohibition. Essentially, the paragraph prohibits the use of force based upon the object sought by its use. Presumably, force which is not used "against the territorial integrity or political independence of another state or in any manner inconsistent with the Purposes of the United Nations" is not prohibited.

The broader view, based upon Article 2(3) and the language in 2(4) regarding the purposes of the United Nations, would preclude any use of force inconsistent with the inherent right of self-defense unless sanctioned by the Security Council. The more limited interpretation is that "any coercive incursion of armed troops into a foreign State without its consent impairs that State's territorial integrity and any use of force to coerce a State to adopt a particular policy or action must be considered as an impairment of that State's political

---

[224] *Id.* Although there are good arguments that the coercive nature of economic measures, for instance, militates in favor of treatment of such measures in the same manner as armed force, this appears to be a minority view. "There can be little doubt that 'use of force' is commonly understood to imply a military attack, an 'armed attack', by the organized military, naval, or air forces of a state; but the concept in practice and principle has a wider significance . . . . Kelsen has asserted that 'use of force' in Article 2, paragraph 4, of the Charter includes both the use of arms and a violation of international law which involves an exercise of power in the territorial domain but no use of arms. It is true that the travaux preparatoires do not indicate that the phrase applied only to armed force: but there is no evidence either in the discussions at San Francisco or in state or United Nations practice that it bears the meaning suggested by Kelsen. Indeed, in view of the predominant view of aggression and the use of force in the previous twenty years it is very doubtful if it was intended to have such a meaning." Ian Brownlie, *Intenational Law and the Use of Force by States*, page 361-362. (1963)

independence."[225] This latter view of Article 2(4) is predominant among States and has support in the decisional law of the International Court of Justice.[226]

Although the UN Charter is the most authoritative source of international law regarding the use of force, there are a couple of additional pieces to the puzzle. In 1970, the UN General Assembly adopted the Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations.[227] In provides, in part:

- "A war of aggression constitutes a crime against the peace for which there is responsibility under international law."
- "States have a duty to refrain from acts of reprisal involving the use of force . . . ."[228]

The last "legislative" piece[229] is the United Nations General Assembly Resolution on the Definition of Aggression.[230] During the drafting of the Charter,

---

[225] Schachter, *International Law in Theory and Practice*, 110-113 (1991), excerpted in Henkin et al., *International Law Cases and Materials*, (1993)
[226] *Id.*
[227] General Assembly Resoution 2625 (1970)
[228] "Reprisals are acts of self-help by the injured State, acts in retaliation for acts contrary to international law on the part of the offending State, which have remained unredressed after a demand for amends. In consequence of such measures, the observance of this or that rule of international law is temporarily suspended, in the relations between the two States. They are limited by considerations of humanity and the rules of good faith, applicable in the relations between States. They are illegal unless they are based upon a previous act contrary to international law. They seek to impose on the offending State reparation for the offence, the return to legality and the avoidance of new offences." *Portugal v. Germany* (The Naulilaa Case), Special Arbitral Tribunal, July 31, 1928.
[229] "A resolution of the General Assembly is not binding under the Charter but is only a recommendation." Michael Reisman and Chris T. Antoniou, *The Laws of War, A Comprehensive Collection of Primary Documents on International Law Governing Armed Conflict*, page 11 (1994) [However, the terms of the resolution is an indicator of opinio juris and may attain the status of customary international law over time.]

the United States had opposed the inclusion of a definition of aggression. The U.S. position was that broad principles as interpreted by the Security Council on a case by case basis, rather than precise definitions, would be more useful in restraining aggression.[231] Subsequently, the U.S. relented to those argued that a definition of aggression would enhance the normative value of Article 2(4).

In 1967, the General Assembly established a Special Committee on the Question of Defining Aggression. The recommendation of the Committee was adopted by the General Assembly in 1974.

Resolution on the Definition of Aggression

Article 1

> Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this definition

Article 2

> The first use of armed force by a State in contravention of the Charter shall constitute prima facie evidence of an act of aggression although the Security Council may . . . conclude that [the use of force was justified.]

---

[230] Resolution on the Definition of Aggression, G.A. Res. 3314 (XXIX), G.A.O.R. 29th Sess., Supp. 31, at 42.

[231] "At the San Francisco Conference on International Organization (1945) there was a movement to insert a definition of aggression in the United Nations Charter. The United States opposed this proposal. It took the position that a definition of aggression cannot be so comprehensive as to include all cases of aggression and cannot take into account the various circumstances which might enter into the determination of aggression in a particular case. Any definition of aggression is a trap for the innocent and an invitation to the guilty. The United States position prevailed at San Francisco and the Charter adopted a system whereby the appropriate U.N. organ, in the first instance the Security Council, would determine on the basis of the facts of a particular case whether aggression has taken place." Annual Report to Congress, President Harry S. Truman, 1950, 5 Whiteman Digest of International Law 740 (1965)

Article 3

Any of the following acts, regardless of a declaration of war, shall subject to and in accordance with the provisions of article 2, qualify as an act of aggression:

(a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however, temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof;

(b) Bombardment by the armed forces of a State by the armed forces of another State or the use of any weapons by a State against the territory of another State;

(c) The blockade of the ports or coasts of a State by the armed forces of another State;

(d) An attack by the armed forces of a State on the land, sea or air forces, marine and air fleets of another State;

(e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;

(f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;

(g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.

Article 4

> The acts enumerated above are not exhaustive and the Security Council may determine that other acts constitute aggression under the provisions of the Charter.

Article 7

> Nothing in this Definition, and in particular article 3, could in any way prejudice the right of self-determination, freedom and independence, as derived from the Charter, of peoples forcibly deprived of that right . . . nor the right of these peoples to struggle to that end and to seek and receive support, in accordance with the principles of the Charter and in conformity with the [Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States

The International Court of Justice (ICJ) had occasion to interpret and apply these principles in *Nicaragua v. United States of America*.[232] The dispute concerned actions taken by, or with the support of, the United States Government within the borders of Nicaragua. The controversial actions included the laying of mines in Nicaraguan ports. Nicaragua asserted that these actions violated the provisions of customary international law that prohibit the use of force by one State against another. The United States took the position that its actions were legal and justified under the principle of self-defense in light of Nicaraguan support of armed opposition movements in neighboring countries, particularly El Salvador.

---

[232] 1986 I.C.J. 1 (June 27, 1986)

The ICJ held for Nicaragua. The court held that self-defense could not be asserted in the absence of an armed attack and the Nicaraguan activities in El Salvador, Honduras and Costa Rica did not constitute an armed attack. For our purposes, it is important to note that the ICJ indicated that there wasn't a *per se* prohibition in customary international law against the introduction of materiel, military instruments included, into the territory of another state.

To summarize, the issue of what actions constitute "force" as the term is used in Article 2(4) has a definite core meaning but remains somewhat unclear around the edges. The term appears to encompass actions involving the application, or threat to apply, armed force designed to deny, without regard to duration, the ability of another State to exercise sovereign control over any aspect of its territory, or to interfere with the exercise or allocation of political power within another State. The majority view is that customary international law defines the term "force" to encompass only armed force, rather than other potentially coercive vehicles of state policy.

With regard to when the use of force is justified, customary international law prescribes that States may use force only under limited circumstances. The exclusive clearly permissible circumstance is individual or collective self-defense. Although the precise contours of this right have been the subject of some contention, it is unarguably available when a State is the victim of an armed attack.[233] States have also claimed, with some success, that humanitarian

---

[233] L. Henkin, Use of Force: Law and U.S. Policy, *Right v. Might*, 37-69 (1989), excerpted in Carter and Trimble, *International Law*, page 1238 (1991)

concerns may justify the use of force. "States have been reluctant to adopt this exception to article 2(4) formally but the legal community has widely accepted that the Charter does not prohibit humanitarian intervention by use of force strictly limited to what is necessary to save lives."[234] In addition, some have claimed a right to use force in support of self-determination. "With colonialism no longer an important concern, the pressure for a 'self-determination exception' to the law of the Charter has subsided, and the potential significance of such an exception, if recognized, is sharply reduced."[235]

If only from a theoretical perspective, it is crucial to understand that the UN Charter did not simply define terms but established a "complex collective security system."[236] The UN Security Council is given the authority to determine, on behalf of the international community, whether the actions of any State constitute a "threat to the peace, breach of peace, or act of aggression."[237] Consequently, the Security Council's competence to condemn and respond to the unilateral acts of States extends beyond the legitimate responsive powers of any single State.

As a practical matter, however, the system has not worked as designed.[238] The fact that this system has not been able to consistently respond to actions

---

[234] *Id.* at 1235.
[235] *Id.* at 1237.
[236] Michael Reisman, Coercion and Self-determination: Construing Charter Article 2(4), 78 A.J.I.L. 642, 642 (July 1984)
[237] UN Charter, Article 39
[238] "The UN Charter's mechanisms often proved ineffective. The situation was reminiscent of the standard American morality play: a town in the "Wild West" in the 19th century without a sheriff, good people, perforce carrying their own weapons and protecting their rights as they see fit. A sheriff comes to town, announcing that he brings with him law and order. As he will henceforth

falling within the scope of its powers, reflects, among other things, "the continuing struggle between the conflicting demands of national sovereignty and international order. . . ."[239] The lack of consistent responsive measures by the UN Security Council makes it difficult to ascribe definite meaning to the fringes of its power. Professor Reisman suggests a consequential analysis that judges coercive acts of States against their effects on legitimate community goals and social order.[240]

2. Factual Scenarios

As should be evident from the preceding discussion, the determination of whether a particular cyber operation is tantamount to an armed attack depends upon, among other things, the general nature, purpose, and scope of the operation. The following scenarios are provided as a general description of various points along a spectrum of activity. In each, it is assumed that, prior to

---

enforce the law, individuals no longer need carry weapons and the town need not tolerate individual resort to force to protect personal rights. Presumably, all good people would be delighted by this constitutional change and would accept the new norm prohibiting the unilateral use of force. Suppose, however, that within six months it becomes clear that the sheriff is utterly incapable of maintaining order. The rule against unilateral force that he has installed may continue on the books, but it is difficult to believe that even the best of citizens will refrain from the techniques of self-help that prevailed before the sheriff's arrival. This, indeed, is what happened in the international system. Within 5 years of the creation of the Organization, a pattern, to be reflected thereafter, was established according to which unilateral violations of Article 2(4) might be condemned but to all intents and purposes validated, with the violator enjoying the benefits of its delict." Michael Reisman, *Coercion and Self-determination: Construing Charter Article 2(4)*, 78 A.J.I.L. 642, 642 (July 1984)

[239] Friedmann, *The Changing Structure of International Law*, pages 254-55 (1964), excerpted in Henkin, *International Law Cases and Materials*, page 897, (1993).

[240] "Coercion should not be glorified, but it is naive and indeed subversive of public order to insist that it never be used, for coercion is a ubiquitous feature of all social life and a characteristic and indispensable component of law. The critical question in a decentralized system is not whether coercion has been applied, but whether it has been applied in support of or against community order and basic policies, and whether it was applied in ways whose net consequences include

the activity described in the scenario, the U.S. and the relevant other State are not in a state of belligerency.

Joint Publication 3-13 sets forth U.S. military doctrine regarding information operations.[241] Computer network attack[242] is just one aspect of information operations. Information operations, as the U.S. military uses the term, can be both offensive and defensive in nature. The following scenarios are completely hypothetical and are simply intended to provide a meaningful context for discussing some of the international legal issues associated with information operations.

(a) Investigation

As noted above, one of the first objectives after identifying the indications and warnings of what appears to be a cyber attack on our information infrastructure is to determine the scope of the intrusion and assess its likely source and objective. In other words, evidence of an unauthorized intrusion prompts an investigation. The investigation typically proceeds by tracing the attack back through the intermediary computers to the source of the attack. In this scenario, the U.S. Air Force traces an attack to a computer in a foreign country and, without authorization from either the owner of the computer, or the State in which it is located, accesses the computer to determine whether it was

---

increased congruence with community goals and minimum order." Michael Reisman, *Coercion and Self-determination: Construing Charter Article 2(4)*, 78 A.J.I.L. 642, 645 (July 1984)

[241] "Actions taken to affect adversary information and information systems while defending one's own information and information systems." Joint Pub 3-13, GL-7 (1998)

[242] "Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." Joint Pub. 3-13, GL-5 (1998)

the source of the attack. The access is obtained exclusively to obtain information and there is no damage done to the computer hardware or software. In addition, the information residing on the computer is not altered.

(b) Active Defense

In this scenario, a non-critical component of the DII is accessed without authorization. The United States determines that the source of the intrusion is a computer located in another State. It is unclear whether the act was sponsored by that State. In response to the intrusion, the Air Force initiates a computer network attack against the source computer with the objective of disabling it as a source of any further attacks.

(c) Computer Network Attack

In this scenario, the United States is the victim of a cyber attack. The attack disables the electrical power and telephone service to the Washington, D.C. metropolitan area for several hours. Another State takes responsibility for the act.

3. Analysis[243]

(a) Investigation

The threshold issue is whether the unauthorized computer intrusion by the United States constitutes an act of force against the State (State X) in which

[243] The analysis is limited to the issues that relate to whether the particular "cyber operation" constitutes a use of force, and if so, whether that force is justified under international law. There are a number of other potential international law issues that might be implicated by these facts. For instance, issues involving the *International Telecommunications Convention of 1982* or the *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space* might arise as we are dealing with the transfer of digital information through satellite and other

the computer is located. Article 3 of the Resolution on the Definition of Aggression (Resolution) lists several acts that are presumptively considered acts of aggression. The unauthorized intrusion does not easily fit into any of the identified categories. The terms of the Resolution contemplate the application of traditional kinetic means of armed force in a manner that interferes with the territorial or political autonomy of a sovereign State.

The computer intrusion does not result in any physical consequences (other than the electronic footprints created by entering the computer). It seems inappropriate to characterize the act of making these footprints as an invasion, attack, bombardment, or otherwise as a use of a weapon. Moreover, not only does the intrusion fail to bring about any of the prohibited consequences, the nature of the intrusion does not evidence any culpable intent.

Although the intrusion is not the legal equivalent of an armed attack, it might constitute an impermissible intervention or unlawful act of coercion. Article 2(4) prohibits actions that violate the territorial integrity or political independence of another State.

It is fair to say that the computer intrusion is a volitional act that results in unauthorized access to something that is physically located within the border of State X. In some respects, the nature of this action is not significantly different from accessing a public website, making a phone call, or sending a fax, to an electronic address that is associated with a physical device located in another

---

communications networks. Moreover, the cyber operations described in the scenarios might violate the domestic laws of the effected State. These issues are beyond the scope of this paper.

State. The intrusion is different from these examples not in the manner of entering the territory of another sovereign, but only at the very end of the link when it involves entering the computer without authorization. Accordingly, the better analogy is not to making the phone call, but tapping into a phone line. Moreover, a computer may be a repository of sensitive information and the unauthorized access might undermine the reliability of the information (whether or not any of it was actually modified or deleted).[244] Arguably, the difference between the role that computers play in our society and that played by other telecommunications devices might justify characterizing the computer intrusion as a violation of territorial integrity. The international community has not specifically addressed this issue. However, the ICJ's suggestions in *Nicaragua v. United States* that logistical support to an opposition group in the territory of another sovereign does not violate international norms, although dicta, tends to cut against a finding that a relatively passive computer intrusion breaches a recognized norm.

In sum, the unauthorized intrusion does not constitute an armed attack which might permit State X to respond proportionally in accordance with Article 51. Nonetheless, it involves actions which are generally only within the province of the sovereign. Consequently, the prudent course, where possible, is to obtain the authorization and cooperation of the government of State X before accessing a computer located in its territory. Clearly, this will not always be an option.

---

[244] Department of Defense, Office of General Counsel, *An Assessment of the International Legal Issues in Information Operations*, 23-24, May 1999.

When it isn't available, and the desire to act remains, the United States must assess the likelihood and adverse consequences of the possible protests, or other diplomatic responses, before acting.

(b) Active Defense

This scenario presents the following issue: under what circumstances does international law permit a State to respond in kind when it is the victim of cyber attack? There are two potential justifications for a response. A state may assert that it is exercising its inherent right of self-defense or that it is undertaking defensive measures under the doctrine of reprisal against State X in response to that state's illegal actions.

As noted above, the right of self-defense under Article 51 seems to be available only when a state has been the victim of an armed attack (or, arguably, when such an attack is imminent.) A cyber attack that has an effect similar to that which could be caused by traditional kinetic weapons could be characterized as an armed attack. For instance, a cyber attack that disabled portions of the air traffic control system, military command and control networks, electrical power distribution systems, or other critical aspects of our information infrastructure, could be characterized as an armed attack. These actions comfortably fit within the proscription in the Resolution on the Definition of Aggression against "the use of any weapon by a State against the territory of another State."[245] The consequences are what control the characterization.

---

[245] Article 3(b), Resolution on the Definition of Aggression

In our scenario, the target is a non-critical component of the DII.[246] There was no loss of life. Unless there was reliable information that further and more significant attacks were imminent, the United States would not be justified in using force against State X on the basis of self-defense.

However, a response under the doctrine of reprisal would be justified. The Restatement (Third) permits a state victim of a violation of an international obligation to execute a proportional response if necessary to terminate the violation or prevent further violations. This is true even if the response might otherwise constitute an unlawful act.[247]

A permissible act of reprisal is premised upon an act that is merely illegal, rather than one that constitutes an armed attack. In this case, the unauthorized intrusion resulted in the intentional disabling of a military asset. Such an act violates the territorial integrity of the United States, is prohibited under customary international law, and, therefore, gives rise to the self-help rights of the victim.

There are several necessary caveats to the conclusion that a responsive cyber attack might be permissible. First, the response must be defensive rather than punitive.[248] Second, it must be proportional. Third, it must be determined

---

[246] Being able to define and recognize the distinction between critical and non-critical is certainly important from a practical perspective. For the purposes of this analysis, a non-critical component is one without which the military readiness of the United States is not impaired.
[247] The Restatement of the Foreign Relations Law of the United States (Third) § 905, "Unilateral Remedies," (1987)
[248] "Armed reprisals do not qualify as legitimate self-defence if they are impelled by purely punitive, nondefensive, motives. But the motives driving States to action are usually multifaceted, and a tinge of retribution can probably be traced in every instance of response to force . . . . To be defensive, and therefore lawful, armed reprisals must be future-oriented, and

that the initial illegal act can be imputed to State X. If the initial intrusion was a private act, as opposed to an act of State, the U.S. should seek assistance from the State. Only when the State refuses to take reasonable measures to terminate the objectionable conduct might the U.S. be justified in self-help.[249]

There is also an issue involving the Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States (Principles Concerning Friendly Relations). It imposes a duty on States to "refrain from acts of reprisal involving force." In this scenario, the initial intrusion, though illegal, was not deemed to be an unlawful use of force giving rise to the right of self-defense. Under the same analysis, a proportional response would not constitute "force" as the term is used in international law. Such a response, therefore, would not run afoul of the Principles Concerning Friendly Relations.[250]

(c) Computer Network Attack

Based upon the preceding discussion, the analysis here is extremely straightforward. As discussed above, a cyber attack that results in substantial, adverse consequences to our nation can properly be treated as an armed attack,

---

not limited to a desire to punish past transgressions." Y. Dinstein, *War, Aggression and Self-Defence* 202-203 (1988)

[249] "The general expectation is that a nation whose interests are damaged by the private conduct of an individual who acts within the territory of another nation will notify the government of that nation and request its cooperation in putting a stop to such conduct." Department of Defense, Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, 26, (May 1999)

[250] If the initial intrusion did constitute an unlawful use of force, then a proportional response would probably be justified as a legitimate act of self-defense.

giving rise to the right of self-defense. Targeting the electrical power and communications links to the national capitol should constitute such an attack.

V. Conclusion

The likelihood of a cyber attack against the nation's information infrastructure is significant; the potential harm to our national security interests from such an attack is substantial. The responsibility for defending against such an attack falls, in part, on the United States Air Force. And, yet, we have not done all that is necessary to ensure that national security organizations, such as the Air Force, are able to effectively respond to information warfare.

The primary federal statutes that establish procedures for conducting searches of computer information were not written to permit an efficient response to information warfare. Consequently, they contain unnecessary, and unintended, hindrances to an effective response to a cyber attack.

The same is true of the Posse Comitatus Act. Although the PCA still reflects an important symbolic truth about the role of the military in domestic civil matters, it fails to account for the nature of a cyber attack. As a result, the PCA imprudently impedes an effective response.

The manner in which the Fourth Amendment applies to governmental responses to cyber attacks needs to be clarified. Although this issue may not present itself in litigation, it is useful for the executive branch to reach an informed conclusion about the limits of its authority.

Finally, with regard to international law, it is essential that we review the manner in which the principles of customary international law regarding the use of force apply in the context of information operations. As customary international law is a constantly evolving doctrine, it is essential that we articulate and implement our policies in a manner that is consistent with the norms that we believe should be adopted by the world community.